Diseño de un plan director de seguridad: estrategia para la protección y mitigación de los riesgos

Claudia Johana Gallego Torres

Asesor

Ever Luis Arroyo Barón

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2026

Dedicatoria

Dedico el presente trabajo de grado inicialmente a mi Dios quien me ha dado la vida.

A mi amado esposo quien ha sido el pilar y el apoyo incondicional que me ha ayudado a continuar en este proceso educativo.

A mi madre que ha sido y siempre será parte de mis logros, al igual que mis hermanos de los cuales siempre he recibido su apoyo en los momentos difíciles.

A mis profesores que se caracterizaron por impartir sus conocimientos de manera clara.

Y a todas aquellas personas que, de una u otra manera han contribuido a mi crecimiento personal y profesional.

Agradecimientos

Dirijo mi agradecimiento en primer lugar a Dios por permitirme llegar a este punto de mi carrera y contar con todos los medios para cumplir con mis objetivos.

Agradezco a mi esposo por su apoyo incondicional y a mi hijo por su gran amor.

Agradezco a los profesores de esta universidad por hacer parte del desarrollo de este proceso y por impartir su conocimiento.

Resumen

Este documento presenta el desarrollo del trabajo de grado aplicado que expone los elementos principales del plan director de seguridad diseñado para la empresa la cual, debido a su deficiencia de medidas de seguridad, se ha visto expuesta a riesgos críticos de seguridad. El ciberataque presentado en el año 2023, que comprometió la información interna y de clientes, evidencio la falta de políticas, procedimientos y herramientas de seguridad, así como la carencia de cultura ciberseguridad a nivel de sus empleados.

La metodología cuantitativa-descriptiva apoyado en la norma 27000 y la metodología Magerit empleada para el desarrollo de este plan director de seguridad, permitió identificar las brechas de seguridad de la compañía donde se evidencio accesos no autorizados, configuraciones incorrectas de aplicaciones, uso incorrecto de contraseñas y prácticas inseguras.

El plan director de seguridad se diseñó siguiendo las fases establecidas (1- Conocer la situación actual de la empresa, 2- Conocer la estrategia corporativa de la organización, 3- Definir proyectos de seguridad, 4- Clasificar y priorizar proyectos, 5- Aprobación del plan director de seguridad).

En base a los hallazgos encontrados se diseñaron políticas de seguridad amparadas bajo la norma ISO 27000 con el fin de proteger los activos de información y garantizando la disponibilidad, integridad y confidencialidad de la información.

Adicionalmente se desarrolló un plan de formación y capacitación en seguridad de la información, expuesto en un manual de funciones de ciberseguridad y temas de formación según la necesidad actual de la compañía.

Palabras clave: Seguridad informática, políticas de seguridad, antivirus, ciberseguridad, phishing, ransomware.

Abstract

This document presents the development of the applied thesis project, outlining the main elements of the security master plan designed for the company, which, due to its deficient security measures, has been exposed to critical security risks. The cyberattack in 2023, which compromised internal and client information, highlighted the lack of security policies, procedures, and tools, as well as the lack of a cybersecurity culture among its employees.

The quantitative-descriptive methodology, supported by ISO 27000 and the Magerit methodology used to develop this security master plan, allowed for the identification of the company's security gaps, revealing unauthorized access, incorrect application configurations, improper password use, and unsafe practices. The security master plan was designed following the established phases (1- Understanding the company's current situation, 2- Understanding the organization's corporate strategy, 3- Defining security projects, 4- Classifying and prioritizing projects, 5- Approval of the security máster plan).

Based on the findings, security policies were designed in accordance with the ISO 27000 standard to protect information assets and guarantee the availability, integrity, and confidentiality of information.

Additionally, an information security training plan was developed, outlined in a cybersecurity job descriptions manual and training topics tailored to the company's current needs.

Keywords: Information security, security policies, antivirus, cybersecurity, phishing, ransomware.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

La seguridad informática se hace cada vez más importante en las organizaciones en el entorno digital y se hace necesario que se establezcan diferentes estrategias que permitan a estas organizaciones a permanecer medianamente seguras ante las diferentes amenazas que se viven diariamente. (Diéguez et al., n.d.)

La compañía, con más de una década de experiencia en el sector de logística de transporte, se enfrenta a grandes desafíos digitales. La estructura operativa de la organización que abarca desde la coordinación de importaciones y exportaciones hasta la gestión administrativa y contable fue vulnerada por causa de un ataque cibernético en el año 2023, causando una gran pérdida de información tanto interna como de clientes, evidenciando la carencia de medidas de seguridad que tiene la empresa.

El anterior incidente presentado por la organización se presentó por la falta de concientización y formación en seguridad informática que poseen sus empleados, ya que se cree que el ataque se inició cuando uno de sus empleados accedió a un enlace malicioso a través de un correo electrónico que recibió. Esta situación crea la importancia y la necesidad de implementar un plan director de seguridad que identifique y aborde los puntos críticos que existen dentro de la organización.

Este plan director de seguridad busca mitigar los riesgos existentes, fortalecer la postura de la seguridad informática de la compañía frente a las posibles amenazas que pueda llegar a presentar y de esta manera garantizar la continuidad de sus procesos operativos y la protección de sus datos sensibles tanto internos como de sus clientes.

Planteamiento del Problema

Antecedentes del Problema

La compañía, con más de una década de experiencia en el sector de la logística de transporte en Colombia, ha enfrentado diversos desafíos en materia de seguridad informática, la ausencia de políticas, procedimientos y controles de ciberseguridad han derivado incidentes que ponen en riesgo la operación interna y la información de sus clientes.

En el 2023 la compañía fue víctima de un incidente significativo, el caso de ransomware afecto datos internos y externos, acompañado por una exigencia económica por el rescate la información. Existen indicios que el ataque se presentó por medio de Phishing, ejecutado cuando un empleado sin tomar precaución accedió a un enlace malicioso recibido por correo electrónico. Este hecho dejo en evidencia la falta mecanismos de protección y la baja de cultura de seguridad que existe en la organización.

La carencia de políticas, procedimientos y herramientas adecuadas mantienen en riesgo la seguridad la organización. Por ello, se hace necesario diseñar e implementar un plan director de seguridad que identifique los puntos críticos de la organización, mitigue los riesgos y fortalezca la capacidad de respuesta frente a futuras amenazas, garantizando así su operatividad y la protección de información propia y la de sus clientes.

Formulación del Problema

En los últimos 5 años, las organizaciones en Colombia se han enfrentado a diferentes ataques cibernéticos, entre los que destacan el acceso abusivo a sistemas informáticos, la suplantación en sitios web, violación de datos personales y hurto. Uno de los incidentes más frecuentes es el secuestro de datos o lo que se conoce como ransomware, especialmente en las empresas que utilizan acceso remoto sin contar con medidas de seguridad. (Álvarez, 2023)

Frente a este panorama, la ciberseguridad ha cobrado gran relevancia, generando en las organizaciones más concientización para tomar medidas de seguridad, conociendo sus riesgos, vulnerabilidades y adoptando medidas que les permitan contrarrestar posibles ataques.

La empresa presenta debilidades de esta índole, evidenciadas en la ausencia de políticas, procedimientos y herramientas adecuadas para la protección de su información y la de sus clientes. El ataque sufrido en el 2023 donde se presume que fue generado por medio de un phishing, derivo en el compromiso de la información sensible y el secuestro de datos, lo cual evidenció la falta de mecanismos de prevención y respuestas de incidentes de ciberseguridad.

Ante esta situación, resulta indispensable la implementación de un plan director de seguridad que permita a la compañía identificar sus riesgos, proteger su información, y responder de manera eficaz a las futuras amenazas, garantizando la continuidad operacional y manteniendo la confianza de sus clientes.

Pregunta Problema

La protección de la información se ha convertido en una prioridad absoluta para las organizaciones. La empresa enfrenta un desafío de salvaguardar sus activos de información frente a las crecientes amenazas cibernéticas de las cuales ya ha sido víctima.

¿Cómo diseñar un plan director de seguridad para la empresa que, en un plazo de un año, permita proteger su información y reducir los riesgos de ciberseguridad que presenta, de acuerdo con la normativa ISO 27000, abarcando su operación en Colombia y teniendo como enfoque políticas de seguridad, procedimientos, controles de ciberseguridad en su infraestructura tecnológica y en la capacitación de sus empleados?

Justificación

Los crecientes ataques de seguridad informática han creado gran preocupación en las diferentes organizaciones, y aunque diversas compañías han tomado diferentes medidas preventivas de seguridad, en algunos casos el tema de ciberseguridad sigue siendo un tema secundario. Según el informe de Fortinet Cyberthreat Predictions for 2024 (Fortiguard, 2024), los ataques cibernéticos especialmente los habilitados por servicios como CaaS, están en aumento debido a la disponibilidad de herramientas más avanzadas. Uno de los sectores más afectado ha sido el financiero y esto se debe la gran cantidad de datos sensibles y transacciones monetarias que se manejan, los ataques son cada vez más sofisticados y veloces siendo así los más frecuentes el phishing y el ransomware. La creación de nuevas técnicas y la utilización de la IA aumentan la vulnerabilidad de los usuarios y entidades.

Es de vital importancia que las compañías entiendan que sin importar el Core que manejan, es necesario que se adopten estrategia de seguridad informática ya que será la a única forma que los riesgos sean más reducidos y controlados (Axentio, 2023).

En este contexto, es fundamental que la compañía, con más de una década de experiencia en el sector de logística de transporte, cuenten con un plan estratégico de seguridad que garantice la continuidad de sus operaciones y la protección de la información interna y de sus clientes.

El plan estratégico de seguridad alineado con la normativa y metodología ISO 27000 y Magerit, permitirá identificar las brechas de seguridad que presenta la organización y priorizar los riesgos más significativos y relevantes, establecerá políticas, procedimientos y controles de seguridad, promoviendo adicionalmente una cultura de seguridad informática en sus empleados por medio planes de formación y capacitación. El plan de seguridad puede contribuir como un modelo de referencia no solo a la compañía sino a las diferentes organizaciones de nuestro país.

Objetivos

Objetivo General

Diseñar un plan director de seguridad para una organización del sector logístico que permita fortalecer la protección de la información, mitigar los riesgos identificados y asegurando la continuidad de sus operaciones.

Objetivos Específicos

Identificar brechas de seguridad informática de la compañía mediante el análisis de sus activos, políticas, procesos y prácticas actuales, con el fin de determinar los riesgos y causas principales.

Diseñar políticas de seguridad alineadas a la normatividad ISO 27000, definiendo lineamientos, controles y procedimientos aplicables a su infraestructura tecnológica y necesidades operativas.

Desarrollar un plan de formación en seguridad de la información, que incluya un manual de funciones y responsabilidades, orientado a promover buenas prácticas y asegurar la correcta aplicación de políticas de establecidas.

Marcos

Marco Referencial

Antecedentes

En los últimos años se ha visto un crecimiento significativo en el sector de logística y transporte debido a la globalización. Este crecimiento ha generado una dependencia hacia las tecnologías como sistemas de gestión de transporte, softwares y algunas plataformas de comunicación digital. Sin embargo, Margi Van Gogh y Felipe Beato en *Foro Económico Mundial*. World Economic, indican que muchas organizaciones no han implementado medidas de seguridad oportunas, lo cual las expones a diferentes vulnerabilidades (Margi Van Gogh, Felipe Beato, 2024).

El informe de World, T. L como proteger el transporte contra amenazas cibernéticas, muestra como estas empresas se han convertido en un blanco debido a los datos de sus clientes, detalles de envíos y documentos financieros (WORLD, 2024).

Estos autores coinciden en que los ataques más comunes como el ransomware y phishing se presentan en estas organizaciones por al no tomar las medidas adecuadas seguridad y no prestar la importancia que requiere el tema de ciberseguridad en las organizaciones.

Teorías

Sistema de Gestión de Seguridad de la Información (SGSI). El SGSI es conocido como un conjunto de políticas y procedimientos que son implementadas por una organización con el fin de proteger su información. El SGSI ayuda a proteger de manera eficaz los pilares de la información que son la integridad, disponibilidad y confidencialidad. El SGSI relaciona puntos importantes dentro de su proceso los cuales son:

- Alineación de TI con el negocio

- Mantener la seguridad de la información
- Garantizar el cumplimento normativo
- Realizar el análisis y ordenar la estructura de los diferentes sistemas de información.
- Establece procesos de trabajo con el fin de mantener la seguridad.

(Rodriguez & Andrés, 2016)

Beneficios de un SGSI. La implementación de un SGSI trae consigo varios beneficios significativos para una organización (Miranda, 2019), seguido se listan algunos de ellos:

- Cumplimiento de normatividad.
- Reduce las incidencias
- Minimiza los riesgos de la seguridad de la información
- Asegura la continuidad del negocio
- Ayuda con la gestión correcta de los activos de información
- Genera confianza en los clientes y socios estratégicos de la organización

Como Implementar un SGSI. Para la implementación de un SGSI existen diferentes formas, pero es de vital importancia adoptar un enfoque que permita cumplir con los elementos que hacen parte de la metodología, según la ISO 27003:2010 existen 5 fases que indican la implementación de un SGSI, (Valencia-Duque & Orozco-Alzate, 2017):

Fase 1: Obtener la Aprobación de la Dirección para Iniciar el Proyecto. En esta fase se contemplan diferentes etapas como el establecimiento de las prioridades de la organización, la definición del alcance del SGSI y la creación del proyecto para aprobación.

Fase 2: Definición del Alcance, Límites y las Políticas del SGSI. En esta fase se establece el alcance y el límite del SGSI y de tecnologías, se define el alcance y limite físico, se

desarrollan las políticas del SGSI y su aprobación, se definen roles y responsabilidades del SGSI.

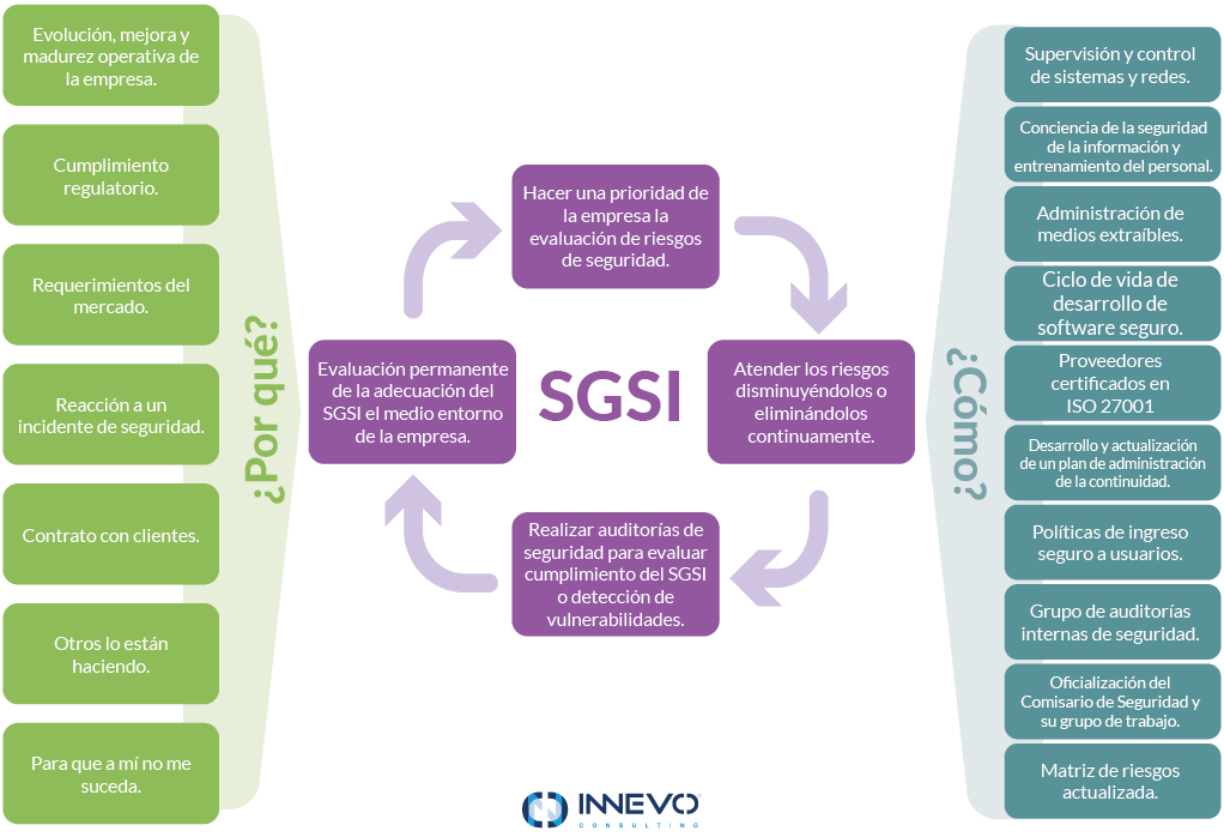
Fase 3: Análisis de los Requisitos de Seguridad de la Información. En esta fase se definen los requisitos de seguridad de la información, se identifican los activos que están dentro del alcance del SGSI y se realiza una evaluación de la seguridad de la información.

Fase 4: Valoración del Riesgo y la Planificación del Tratamiento. En esta fase se genera la valoración del riesgo, se establecen los controles de los riesgos y se busca una siguiente aprobación para que el SGSI sea operable.

Fase 5: Diseñar el SGSI. En esta fase se procede con el diseño del SGSI teniendo en cuenta el diseño de la seguridad de la información, seguridad física y tecnológica, el diseño especifico de un SGSI y la producción de un proyecto final del SGSI.

Figura 1

Mejora Continua del SGSI



Nota. Imagen obtenida de https://blog.innevo.com/que-es-sgsi

Familia de la ISO 27000. La serie de la familia ISO 27000 tiene como objetivo establecer buenas prácticas en todo lo que concierne a la seguridad de la información, orientado a la mejora continua y la mitigación de riesgos. (Icontec, 2022)

Norma ISO/IEC 27001. Esta norma contiene los requisitos para la implementación, mantenimiento y mejora continua de un SGSI.

Norma ISO/IEC 27002. Ofrece una guía para la creación de controles de seguridad y es un complemento de la ISO 27001.

Norma ISO/IEC 27005. Ofrece recomendaciones para la gestión de riesgos. Esto hace referencial análisis para planificación, ejecución y seguimiento a las medidas establecidas.

Norma ISO/IEC 27008. Contiene los controles de seguridad de la información y suministra orientación a los auditores acerca de la implementación y operación de controles.

Figura 2

Familia ISO 27000

Nota. Familia de la ISO 27000, Imagen obtenida de https://victorsinuco.blogspot.com/2017/06/

Plan Director de Seguridad. Un plan director de seguridad es una estrategia integral que busca gestionar y proteger los activos de información de una organización. Esto se logra con la priorización de un conjunto de proyectos relacionados con la seguridad con los cuales se busca reducir los riesgos que presenta la organización. (Hostetler & Hostetler, 2011)

Fases de un plan director de seguridad

Un plan director de seguridad está compuesto por 6 fases cíclicas basadas en la mejora continua.

FASE 1 Conocer la situación actual de la empresa: En la fase 1 se busca conocer el estado actual de la empresa en relación con la ciberseguridad. Esta fase reúne a todos los actores incluyendo a los directivos garantizando los recursos y alineación con los objetivos estratégicos de la compañía.

FASE 2 Conocer la estrategia de la compañía: Esta fase busca conocer la estrategia corporativa de la organización, se busca conocer los proyectos actuales de la organización y los futuros. Esta fase también busca alinear la estrategia de seguridad a nivel de TIC y la estrategia general del negocio.

FASE 3 Definición de proyectos e iniciativas: Después de obtener la información de las fases anteriores se definirá las iniciativas y proyectos que se requieren para alanzar el nivel de seguridad que requiere la organización.

FASE 4 Clasificación y priorización de proyectos: Después de definir los proyectos en la fase anterior, en esta fase se realizará la clasificación y priorización teniendo en cuenta su costo y el tiempo de desarrollo.

FASE 5 Aprobación del plan director de seguridad: En esta fase se realiza la aprobación del plan director de seguridad por parte de los directivos de la organización. Se pueden presentar

correcciones donde se finalice con diferentes ajustes y posterior aprobación por parte de los directivos.

FASE 6 Implementación del plan director de seguridad: Una vez se genera la aprobación por parte de los directivos el plan director de seguridad es puesto en marcha.

Marco Conceptual

Plan Director de Seguridad

El plan director de seguridad se entiende como la definición y la priorización de proyectos orientados a la protección de la información y la reducción de riesgos que presenta una organización (Ciberseguridad, n.d.). Estos proyectos se diseñan según las necesidades primarias de la empresa y teniendo en cuenta el tamaño de la organización, su sector empresarial y el avance tecnológico (Gonzáles & Méndez, 2021):

Un aspecto clave de un plan director no solo el enfoque técnico de seguridad, sino también en la cultura de seguridad sostenible en sus empleados, que abarque de forma vertical, desde la alta dirección hasta involucrar todos los niveles de la organización. (Davies & Fennelly, 2019).

Aunque algunos autores muestran el plan director de seguridad con un objetivo estratégico y a largo plazo, otros como la norma ISO 27000 buscan la forma que se integre con todos los procesos de negocio con el fin de generar más efectividad.

Ciberseguridad

ISACA define a la ciberseguridad como la Protección de activos de información, por medio del tratamiento de amenazas y que ponen en riesgo la información (Infosecurity, n.d.). Su propósito central es garantizar la protección de los activos organizacionales y usuarios.

La ciberseguridad debe alinearse con diferentes estándares internacionales como NIST y

la ISO 27001, ampliamente adaptables a empresas de distintos sectores. (Ibrahim, 2021) Valkenburg y Bengiovanni en El artículo Unravelling the three lines model in cybersecurity: a systematic literature review indican que la gobernanza de la ciberseguridad en tres líneas de defensa que son equipos IT y ciberseguridad quienes diseñan e implementan controles de seguridad, intermediarios y asesores de la implementación los cuales supervisan los riesgos y el cumplimiento de las políticas y la auditoría interna la cual se encarga de evaluar las dos líneas anteriores. (Valkenburg & Bongiovanni, 2024).

Seguridad de la Información

La seguridad de la información busca proteger los sistemas y datos de amenazas que pongan en riesgo su integridad, confidencialidad y disponibilidad (Cloudflare, n.d.).

La seguridad de la información busca reducir los riesgos y es por esta razón que se busca medidas que permitan salvaguardar la información de manera segura (Mosquera Amancio, n.d.).

Los autores coinciden con la definición y protección a nivel los tres pilares de la información.

Seguridad Informática

La seguridad de la información se encuentra relacionada con la protección de los sistemas TI como lo son los hardware, software, documentación digital. Es conocida también como un activo estratégico dentro de la organización. (Valencia-Duque & Orozco-Alzate, 2017)

Pilares Seguridad de la Información

Según la ISO 27001 (Icontec, 2022) existen tres pilares en la seguridad de la información que son confidencialidad, disponibilidad e integralidad con los cuales se busca garantizar la adecuada gestión de la información.

A continuación de describen pilares de la información (Aceves, n.d.-a).

Confidencialidad. Hace referencia al acceso a la información que solo pueden tener las personas autorizadas. (Fabiana Meijon Fadul, 2019)

Disponibilidad. Hace referencia a que la información debe estar siempre disponible y accesible en el momento adecuado y desde cualquier medio tecnológico. (Christian & Ochoa, 2018)

Integridad. Busca que la información no se encuentre alterada y no tenga modificaciones que alteren su validez. (Christian & Ochoa, 2018)

Vulnerabilidades. Las vulnerabilidades son conocidas como las debilidades en los sistemas, procedimientos o controles de seguridad que pueden ser explotados por atacantes. Las vulnerabilidades pueden ser técnicas o humanas.(Smowl, 2024)

Phishing. Es conocido como una técnica de ingeniería social por medio de la cual un atacante engañan a un usuario para que revelen información confidencial que pueden ser usuarios, contraseñas. Esta técnica de ataque se genera mediante correos electrónicos o sitios web falsos.(Kosinski, 2024)

Ransomware. Este es un tipo de malware el cual se encarga de cifrar la información de las víctimas y posteriormente exigiendo un rescate por la información. Este tipo de ataque se ha considerado como uno de los más destructivos.(IBM, 2023)

Activos de Información. Los activos de información son la información o recursos importantes para una organización y que son fundamentales para sus operaciones. Los activos de información requieren de controles de seguridad y estos pueden presentar un costo para las organizaciones.

Marco Teórico

El presente marco teórico reúne los fundamentos conceptuales y normativos que

sustentan el diseño de un plan director de seguridad para una organización del sector logístico. Se busca integrar las principales teorías de seguridad de la información, analizando sus aportes, limitaciones y compararlas con enfoques alternativos que permitan contextualizar su aplicabilidad en organizaciones.

Teoría Principal

Conceptos Fundamentales de la Seguridad. La seguridad de la información busca la protección de todos los tipos de información y activos por medio de principios esenciales como la confidencialidad, integralidad y la disponibilidad, conocidos como la triada CIA (Rawat, 2023a)

Confidencialidad. Mantener la información de manera segura, accesible solo a personal autorizado. Algunos controles que se usan para cumplir con este principio son la identificación, autenticación, autorización y la encriptación.

Integridad. La integralidad busca que los datos no sufran alteraciones, garantizando que información sea precisa y completa.

Disponibilidad. Asegura que la información esté disponible para aquellas personas que cuentan con la autorización para acceder a ella.

Aunque algunos autores como (Rawat, 2023b) y (López, 2017b) coinciden en la importancia de la triada, para algunos autores como (Aceves, n.d.-b), indica que los conceptos de la triada resultan insuficientes frente a las amenazas actuales.

ENISA (Lella, n.d.)indica que, en entornos empresariales digitalizados, la disponibilidad se refiere no solo a un acceso inmediato de la información sino a la continuidad operacional de los servicios críticos, esto implicaría que la seguridad de la información debería integrase con planes de seguridad.

Logros de la Triada. La triada es ampliamente adoptada en las normas y marcos como ISO 27001, NIS y COBIT, lo cual confirma su relevancia e importancia en la seguridad de la información. Según lo indicado por (Von Solms & Van Niekerk, 2013), la simplicidad de la triada facilita a las compañías que presentan un déficit de madurez en seguridad, puedan comprender la esencia de la protección de datos.

Limitaciones. Algunos autores como (Mamami et al., 2023)indican que la triada se hace insuficiente ante las amenazas actuales ya que es posible abordar algunos aspectos como la privacidad, autenticidad y trazabilidad. Otros autores como (Tzavara & Vassiliadis, 2024) indica que el concepto de ciberseguridad debe ser más amplio que solo el hecho de basarla en la confidencialidad, integridad y disponibilidad.

Si bien existe un consenso de la importancia de la triada, aún existen vacíos de como las compañías no tecnológicas adaptarían los conceptos de la triada CIA a sus procesos tecnológicos. Las propiedades de la triada en entonos relevantes como la IoT, IA e infraestructuras críticas no son suficientes según lo indicado (Lundgren & Möller, 2017), por lo anterior es necesario agregar al plan director de seguridad y referencia a la triada factores como trazabilidad, continuidad y controles tanto humanos como técnicos.

Algunos modelos más amplios como el modelo Parkerian Hexad (Pender-Bey, n.d.) muestra una propuesta para superar las limitaciones de la Triada, esas propuestas se basan en incluir conceptos como (Posesión/Control, Autenticidad y Utilidad), se indica la inclusión de estos conceptos ya que Parker describe que la triada es demasiado básica para abarcar los riesgos modernos.

Teniendo en cuenta los modelos básicos descritos anteriormente se debe ofrecer un modelo que busque ofrecer una estructura que responda a las necesidades actuales. Algunos

componentes deben ser:

Tener una seguridad integral: Se debe involucrar temas como datos, personas, procesos y además la tecnología. Esta seguridad debe adaptarse a los cambios tecnológicos, a las amenazas actuales y las venideras.

La confidencialidad debe ir más allá del acceso no autorizado, como incorporar un el cifrado en tránsito, controles de privilegios y doble autenticación. En la integralidad de se debe tener en cuenta el lugar, dispositivo y comportamiento, y para la disponibilidad se propone tener recursos indispensables de duplicados y respaldos, implementar también mecanismos estrictamente necesarios con el fin de que la operación continue sin interrupción.

Normativa y Estándares

Existen obligaciones claves que pueden ser de gran importancia para la empresa como lo son: (Congreso de Colombia, 2012).

Ley 1581 del 2012-Ley de protección de datos personales: Las compañías deben implementar medidas de seguridad adecuadas para proteger los datos personales, cumpliendo con la normativa y manteniendo los pilares de la información. Algunas medidas que se pueden implementar son el cifrado de datos, gestión de accesos y auditorias periódicas.

Ley 1581 del 2012 (Articulo 17)-Notificación de incidentes: Las compañías tienen la obligación de reportar los incidentes de seguridad que afecten los datos personales, ante las entidades correspondientes y a los afectados.

Ley 1273 de 2019 - Ley de delitos informáticos: Constituye una serie de delitos informáticos y sus sanciones, contiene medidas para la prevención y la mitigación de los ataques cibernéticos.(Andrés Jiménez-Almeira & López, 2023)

La norma ISO 27000 contiene diferentes normas que ayudan a la con la gestión de la

seguridad de la información y que puede ser crucial en el proceso que requiere la compañía, (Icontec, 2022).

ISO/IEC 27001: Esta norma específica los requisitos para la implementación o mejora de un SGSI (Sistema de Gestión de la seguridad de la información).

ISO/IEC 27002: Es una guía de buenas prácticas donde se ofrece una guía para la creación de controles de seguridad.

ISO/IEC 27003: Ofrece una ayuda para la implementación un SGSI incluyendo el método PHVA (Planear, Hacer, Verificar y Actuar).

ISO/IEC 27004: Especifica la medición de la eficacia del SGSI y sus controles.

ISO/IEC 27005: Ofrece recomendaciones para la gestión de riesgos. Esto hace referencia al análisis para la planificación, ejecución y seguimiento a las medidas establecidas.

Marco COBIT: El marco COBIT es un marco de gestión y gobernanza de TI que ayuda a implementar la gobernanza de la tecnología de la información TI y la ciberseguridad, tiene como objetivos gestionar y mitigar los riesgos referentes a la ciberseguridad. (Eito-Brun & Calleja Aliaga, 2020).

Aunque los lineamientos técnicos y de gobernanza de la norma ISO 27000 y Cobit se presentan supremamente estructurados no se puede evidenciar la existencia de su aplicabilidad en empresas pequeñas donde sus recursos financieros y de personal son limitados.

Gestión de Riesgos

Existen diferentes metodologías y normas para la gestión de la seguridad de la información orientadas a proteger los activos de información de una organización. Estas buenas prácticas pueden ser combinadas teniendo como resultado un marco de seguridad integral y adaptables a la organización.

Algunas de estas metodologías y normas son conocidas como el marco de referencia NIST, la ISO/IEC 27001 y Magerit.(Barraza de la Paz et al., 2023).

Algunos elementos claves en la gestión del riesgo son: (Kassa, 2017)

Evaluación del riesgo: Se realiza la identificación de amenazas, vulnerabilidades y las consecuencias que puede afectar la seguridad de la información.

Tratamiento del riesgo: Se definen las acciones para mitigar, transferir o aceptar los riesgos identificados.

Análisis de impacto en el negocio: Se identifican los activos que críticos y el impacto que puede presentar si se afectan.

Ciclo de vida de los riesgos: Se realiza la identificación, evaluación, monitoreo y la revisión continua del riesgo.

Políticas de Seguridad de la Información

Las políticas de seguridad de la información es un conjunto de reglas y procedimientos que tienen como objetivo proteger los activos de la organización. (Outpu, 2021)

Política general de la seguridad: Hace referencia a un documento estratégico que define la postura de la organización en relación con la protección de la información y busca garantizar que se cumplan los pilares de la información.

Política de gestión de incidentes: Se generan directrices para la identificación, respuesta y recuperación ante incidentes de seguridad.

Política de gestión de accesos y control de identidades: Se incluyen las directrices necesarias para la administración de privilegios para el acceso a la información y a los sistemas.

Política de Backup y recuperación: Se generan estrategias para garantizar la disponibilidad de la información con el fin de garantiza la continuidad del negocio.

Marco de Implementación

Definición de roles y responsabilidades: Se realiza la asignación de roles y responsabilidades para la implementación, monitoreo y el cumplimiento del plan director de seguridad. (Epa & Information, 2016)

Plan de capacitación y concientización: Se definen estrategias para la capacitación del personal.

Monitoreo y auditoria: se realizan controles de seguridad con el fin de auditar el cumplimiento de las políticas y los procedimientos.

Fases Para el Plan Director de Seguridad

INCIBE (Instituto Nacional de Ciberseguridad) (INCIBE, n.d.), establece un marco solido para la elaboración de un plan director de seguridad donde se detallan 6 fases para su desarrollo.

Fase 1- Conocer la Situación Actual de la Empresa. En esta fase se pretende conocer la situación que presenta la compañía referente a su seguridad informática por medio de actividades como:

***Actividades Previas-Fase1*.** Acotar y establecer el alcance: En esta actividad se deberá definir y acotar el alcance, donde se tendrá en cuenta activos y procesos críticos. Se deberá priorizar aquellos activos y procesos sin los cuales la compañía no podría operar.

Responsables de la gestión de los activos: En esta actividad se busca definir y asignar roles y responsabilidades específicas para la gestión de los activos. Esta actividad se desarrolla identificando los activos y asignando los responsables; teniendo en cuenta que este caso por ser una compañía pequeña, varias responsabilidades pueden recaer sobre una sola persona.

Valoración Inicial: El objetivo de la valoración inicial es realizar un diagnóstico

preliminar de la situación actual de la empresa en términos de seguridad informática. Esta valoración se realiza en diferentes actividades:

Evaluación de controles existentes

Se realiza el análisis del cumplimiento normativo

Se evalúa el grado de madurez de los controles

Se realiza un documento de controles donde se enumera los controles aplicables y su estado de implementación (Declaración de aplicabilidad- SOA)

Se debe realizar reuniones con los responsables de las áreas con el fin de recopilar información y evaluar el cumplimiento de controles.

Inspeccionar las instalaciones físicas donde se verifican controles físicos, accesos y condiciones de las áreas donde se almacenan datos sensibles.

Con esta actividad se espera obtener una visión global de los controles implementados en la empresa y un listado inicial de debilidades y oportunidades de mejora, que servirán como base inicial.

Análisis de cumplimiento: En esta actividad se busca evaluar el nivel de cumplimiento de controles de seguridad establecidos por la empresa, con respecto a normativas, estándares y requisitos internos.

Lo anterior permitirá identificar brechas y establecer prioridades para la mejora de la seguridad.

Algunas actividades para realizar el análisis del cumplimiento son:

Generar reuniones con personal clave de la organización y evaluar el nivel de cumplimiento actual de seguridad establecidos.

Usar estándares internacionales como la ISO 27002 con el fin de encontrar controles

aplicables y compáralos con los establecidos por la organización.

Usar checklist y formularios para registrar las evidencias del cumplimiento y posteriormente clasificar el incumplimiento.

Se realiza un documento con los hallazgos encontrados donde se registran los problemas, deficiencias y evidencias encontradas.

Teniendo en consideración para la empresa y dado a que no se cuenta con ningún sistema de seguridad establecido se realiza un enfoque en áreas críticas como:

- Protección de datos sensibles.
- Implementación de medidas básicas antivirus y políticas de contraseñas.
- Copias de seguridad de la información.

***Establecer los Objetivos*.** Esta actividad tiene como propósito definir las metas claras y específicas que la empresa debe alcanzar en materia de ciberseguridad. Lo anterior permitirá enfocar lo esfuerzos hacia las áreas críticas y de esta forma alinear las iniciativas del plan director de seguridad con las necesidades de la empresa.

Algunas de las actividades que se realizan para establecer los objetivos son:

Analizar la información recopilada donde se revisan los resultados del análisis del cumplimiento, la valoración inicial y el análisis de riesgos.

Se definen objetivos específicos de mejora que sean medibles y alineados a la necesidad de la compañía y deben estar relacionados con la protección de los activos críticos, reducción de riesgos inaceptables, cumplimiento normativo y el fortalecimiento de la cultura de la ciberseguridad.

***Análisis Técnico de Seguridad*.** Esta actividad tiene como objetivo evaluar el estado actual de los sistemas y controles técnicos que tiene la compañía para identificar deficiencias y

áreas de mejora en la infraestructura tecnológica.

Algunas actividades para el análisis técnico de seguridad son:

Revisión de los controles técnicos existentes donde se evalúa si existen y funcionan.

Se realiza la comprobación de la infraestructura tecnológica verificando la seguridad de la red, seguridad en servidores y sistemas críticos y los controles de acceso físico.

Realización de pruebas técnicas donde se llevarán a cabo auditorias con el fin de detectar vulnerabilidades en los sistemas.

Evaluación del impacto de las deficiencias encontradas y como estas afectan la seguridad de la información.

Registro de hallazgos, aquí se realiza la documentación de los hallazgos donde se documenta la vulnerabilidad y su impacto, adicional se prioriza el hallazgo según su criticidad.

Con el análisis técnico se espera obtener un documento detallado de las deficiencias técnicas encontradas, vulnerabilidades críticas y las recomendaciones técnicas.

***Análisis de Riesgos*.** Esta actividad busca evaluar y priorizar los riesgos a los que está expuesta la compañía, con base a sus activos de información y las amenazas que pueden presentar.

Algunas actividades para llevar a cabo el análisis de riesgos son:

- La identificación de los activos de información
- La identificación de amenazas y vulnerabilidades
- Evaluar controles existentes
- Clasificar y priorizar los riesgos-Nivel del riesgo aceptable
- Proponer estrategias del tratamiento del riesgo.
- Debido a que la compañía no cuenta con medidas de seguridad actuales este

análisis se realizara en base a la identificación de los riesgos más críticos asociados a la falta de controles básicos de seguridad informática.

Fase 2- Conocer la Estrategia Corporativa de la Organización. Esta fase busca conocer la estrategia corporativa de la organización alineando las medidas de la seguridad de la información con la estrategia general de la empresa.

Algunas actividades que se tendrán en cuenta para esta fase son:

- La identificación de la estrategia corporativa.
- Evaluar las implicaciones para la seguridad teniendo en cuenta la estrategia corporativa
- Alinear la seguridad con la estrategia de negocio.
- Involucrar las áreas claves de la organización.
- La ejecución de esta fase permitirá obtener un entendimiento claro de los objetivos estratégicos de la compañía con el fin de tener un enfoque alineado a la seguridad de la información.

Fase 3- Definición de Proyectos de Seguridad. Esta fase permite definir acciones, iniciativas y proyectos necesarios que permitan alcanzar un nivel de seguridad requerido por la organización.

Teniendo en cuenta que la empresa no cuenta con medidas de seguridad informática se realizaran actividades específicas que ayuden a definir los proyectos de seguridad que se requiere.

***Definir Iniciativas Esenciales*.** Estas iniciativas priorizaran proyectos con bases de un entorno seguro.

- Involucrar la dirección para la validación y aprobación de los proyectos.

- Limitar los recursos diseñando iniciativas alcanzables considerando los recursos actuales de la empresa.
- La definición de los proyectos se realizará en base a la estrategia de la organización.
- Como resultado de esta fase se espera determinar iniciativas que aborden las deficiencias de seguridad actuales que presenta la empresa.

Fase 4- Clasificar y Priorizar los Proyectos. En esta fase se debe organizar y priorizar los proyectos e iniciativas identificados en la fase anterior, algunos criterios para tener en cuenta para esta clasificación según la situación de la empresa son:

- Priorizar proyectos que mitiguen los riesgos más críticos.
- Identificar proyectos que tengan bajo esfuerzo, pero un alto impacto.
- Los proyectos deben estar alineados con la estrategia corporativa.
- Evaluar los costos y recursos que requiere cada proyecto.
- Como resultado de esta fase se tendrá una lista estructurada y priorizada de proyectos estratégicos, claros y de gran valor para la seguridad de la información de la organización.

Fase 5- Aprobación del Plan Director de Seguridad. Esta fase busca la aprobación formal por parte de la gerencia del plan director de seguridad, antes de pasar por diferentes revisiones y ajustes pertinentes.

La dirección realiza el análisis del alance, la duración y la prioridad de los proyectos definidos, y es posibles que se soliciten ajustes. Después de que se realicen ajustes al documento este debe pasar nuevamente por revisión, este proceso puede repetirse varias veces hasta lograrla aprobación por parte de la gerencia o dirección de la empresa.

Fase 6- Puesta en Marcha. En esta fase se ejecutan las acciones y proyectos definidos y aprobados, siguiendo un enfoque estructurado que permita garantizar el cumplimiento de los objetivos.

Algunas actividades para esta fase son:

- Presentación inicial del proyecto
- Asignación de responsables
- Seguimiento al plan director de seguridad
- Revisión de avances
- Ajustes continuos al plan director de seguridad

Marco Legal

Las empresas de logística de transporte no se dedican a mantener una seguridad informática continua en sus procesos y es por esto por lo que la inversión en el aseguramiento de sus activos es muy poca o casi nula, lo cual hace que se encuentren en un riesgo constante de ser atacadas por las vulnerabilidades de seguridad informática que presentan.

Los estándares establecidos para los procesos de buenas prácticas de seguridad de la información ayudan a las organizaciones a proteger sus activos de la información y conlleva a que la se cumpla con los pilares de la información en su confidencialidad, integridad y disponibilidad. (Arroyabe et al., 2024)

Las organizaciones poseen ciertas responsabilidades y obligaciones referentes a la seguridad informática. Tienen la responsabilidad de generar medidas técnicas y organizativas que protejan los datos de sus clientes y adicional deben ser propicios a reportar los incidentes que se presenten y que involucren la información de terceros. (Arcos-Argudo et al., 2023)

Existen obligaciones claves que pueden ser de gran importancia para la empresa como lo

son: (Congreso de Colombia, 2012)

Ley 1581 del 2012-Ley de protección de datos personales: Las compañías deben implementar medidas de seguridad adecuadas para proteger los datos personales, cumpliendo con la normativa y manteniendo los pilares de la información. Algunas medidas que se pueden implementar son el cifrado de datos, gestión de accesos y auditorias periódicas.

Ley 1581 del 2012 (Articulo 17)-Notificación de incidentes: Las compañías tienen la obligación de reportar los incidentes de seguridad que afecten los datos personales, ante las entidades correspondientes y a los afectados.

Ley 1273 de 2019 - Ley de delitos informáticos: Constituye una serie de delitos informáticos y sus sanciones, contiene medidas para la prevención y la mitigación de los ataques cibernéticos.(Andrés Jiménez-Almeira & López, 2023)

La norma ISO 27000 contiene diferentes normas que ayudan a la con la gestión de la seguridad de la información y que puede ser crucial en el proceso que requiere la compañía, (Icontec, 2022).

ISO/IEC 27001: Esta norma específica los requisitos para la implementación o mejora de un SGSI (Sistema de Gestión de la seguridad de la información).

ISO/IEC 27002: Es una guía de buenas prácticas donde se ofrece una guía para la creación de controles de seguridad.

ISO/IEC 27003: Ofrece una ayuda para la implementación un SGSI incluyendo el método PHVA (Planear, Hacer, Verificar y Actuar).

ISO/IEC 27004: Especifica la medición de la eficacia del SGSI y sus controles.

ISO/IEC 27005: Ofrece recomendaciones para la gestión de riesgos. Esto hace referencia al análisis para la planificación, ejecución y seguimiento a las medidas establecidas.

Marco COBIT: El marco COBIT es un marco de gestión y gobernanza de TI que ayuda a implementar la gobernanza de la tecnología de la información TI y la ciberseguridad, tiene como objetivos gestionar y mitigar los riesgos referentes a la ciberseguridad. (Eito-Brun & Calleja Aliaga, 2020).

Marco contextual

Nombre de la Empresa

Reseña

La empresa fue constituida en el año 2014 en la ciudad de Bogotá, dio sus inicios como una empresa de servicios de transporte terrestre, después de algún tiempo continuo con servicios de transporte aéreo y marítimo. En sus inicios esta compañía comenzó con dos empleados encargados de realizar todo los procesos operativos y administrativos, hoy en día cuenta con más de 8 empleados que ayudan con los diferentes procesos organizacionales de la compañía.

Política de Calidad

Tiene el compromiso de cumplir con las normas que rigen sus procesos y que sus clientes se sientan confiados y satisfechos con los procesos que se realizan para cumplir con el transporte de sus mercancías.

Naturaleza Jurídica

La compañía es una empresa jurídica de sociedad por acciones simplificada (S.A.S).

Ubicación Física

La empresa se encuentra ubicada en la ciudad de Bogotá-Localidad de Fontibón, centro comercial fiesta Fontibón.

Diseño Metodológico

Tipo de Investigación

Cuantitativa-Descriptiva

El libro Security Metrics: Replacing Fear, Uncertainty, and Doubt indica la importancia de la medición cuantitativa en la seguridad informática. Señala que las métricas deben ser: (Andrew Jaquith, n.d.)

Consistentes: Medibles de manera repetitiva.

Representativas: Donde se reflejen aspectos claves de la seguridad informática.

Prácticas: Deben ser comprensibles y aplicables para la toma de decisiones.

En el presente proyecto aplicado se utilizará la investigación cuantitativa-descriptiva, con la cual se utilizarán herramientas informáticas y matemáticas para obtener resultados concluyentes y precisos en el análisis de datos.

El tipo de investigación cuantitativa-descriptiva se utiliza para analizar y describir la situación actual de seguridad informática de la empresa, evaluando los aspectos más relevantes como las vulnerabilidades y las brechas de seguridad identificadas. Este enfoque permite describir la realidad de situaciones y eventos específicos, con el fin de comprenderlos y realizar propuestas concretas para la solución.

Por medio de esta metodología se analizarán diferentes componentes claves de la seguridad de la información en la compañía, incluyendo políticas de seguridad actuales, procedimientos existentes, herramientas implementadas, y prácticas ejecutadas por los empleados. Los resultados obtenidos ayudaran a identificar las áreas críticas, con el fin de diseñar procesos y mecanismos que fortalezcan la protección de los activos de información alineándose con los estándares establecidos en la norma ISO 27001 y Magerit.

Recolección de la Información

La recolección de información se realizará por medio de un análisis descriptivo fundamentado en el estudio de información secundaria. Según lo indicado por Eliana Gallardo (Gallardo, 2017), la información secundaria se hace referencia a datos obtenidos por otras fuentes por medio de contacto indirecto con el objeto de estudio.

La recolección de información para la organización se recurrirá a:

Informes internos de auditorías y procesos administrativos.

Análisis de incidentes previos: Realizar los análisis previos de incidentes de ciberseguridad ayuda con la identificación de patrones de ataques y áreas críticas las cuales requieren de una atención rápida.

El libro Digital Evidence and Computer Crime (Kizza & Migga Kizza, 2011) destaca la importancia de analizar los ataques cibernéticos con el fin de comprender las tácticas de los atacantes y las debilidades explotadas.

La aplicación de normativas y técnicas como la ISO 27001 y Magerit ayudarán a comprender el estado actual de la organización y serán de guía para la generación del plan director de seguridad gracias a que ofrecen un enfoque estructurado de seguridad de la información.

Instrumentos de Recolección de Información

Algunos instrumentos de recolección de información que serán utilizados son:

Matriz de análisis de riesgos: Permitirá identificar las amenazas, vulnerabilidad y activos críticos de la compañía.

Checklists de control interno informático actual ISO 27001 y Magerit.

Revisión documental de políticas de seguridad establecida en la compañía.

Técnicas de Análisis

Las técnicas de análisis utilizadas para el plan director de seguridad son:

Análisis de contenido aplicado: Este análisis se realiza a los informes internos y de documentación corporativa, examinado de manera sistemática y objetiva con el fin de identificar temas relevantes de seguridad.

Clasificación y valoración de las vulnerabilidades y valoración del riesgo en base a la metodología magerit: Esta valoración se realizará de manera cuantitativa teniendo en cuenta la autenticidad, trazabilidad, confidencialidad, integridad y disponibilidad de los activos de información.

Análisis de riesgo cualitativo: Se evaluará cada brecha de seguridad según su impacto y probabilidad.

Criterios de Validación

Los criterios de validación establecidos tienen como fin, asegurar la rigurosidad de la metodología y la confiabilidad de los resultados obtenidos durante el desarrollo del análisis de riesgos por medio de la metodología Magerit, los criterios de validación establecidos garantizan la calidad de los datos y la coherencia del proceso.

Fiabilidad de datos: La información que se usara debe venir de fuentes oficiales confiables como la documentación y datos propios de la compañía.

Información actual: Se validará la información actuar de incidentes de seguridad ocurridos en los últimos tres años.

Muestra representativa: La información recolectada debe relacionar todas las áreas de la compañía.

Objetividad en la medición: Los resultados serán obtenidos por medio de escalas

numéricas y categorías según la metodología Magerit como (Niveles de madurez 0-5, niveles de impacto y probabilidad del riesgo).

Validez de instrumento de medición: Se validan los instrumentos utilizados como matrices, encuestas o listas de validación, con el fin de medir de forma precisa el nivel de riesgo y el grado de madurez de los controles.

Consistencia interna: Se valida que la metodología Magerit y COBIT contengan coherencia entre los criterios de riesgo, los tipos de controles y los niveles de madurez.

Desarrollo Plan Director de Seguridad

Desarrollo Objetivo 1 - Fase 1 Conocer la Situación Actual de la Empresa

Objetivo Específico 1

Identificar las brechas de seguridad informática de la compañía, mediante el análisis de sus políticas y prácticas actuales, con el fin de diagnosticas los riesgos y causas específicas.

Alcance

El plan director de seguridad para la empresa abarca la identificación y evaluación de los activos, de los procesos y los recursos relacionados con la seguridad de la información de la compañía, con el objetivo de establecer un diagnóstico claro de la situación actual en referencia a la seguridad informática.

El presente proyecto abarca el diseño, estructuración y validación teórica del plan director de seguridad, siguiendo las directrices establecidas hasta la fase 5, que corresponde a la aprobación del plan director de seguridad por parte de la empresa.

La fase 6 corresponde a la puesta en marcha del plan director de seguridad la cual no se encuentra contemplada dentro del alcance de este proyecto, ya que su desarrollo depende de decisiones y recursos que son propios de la organización.

Áreas Incluidas

Oficina física (Bogotá)

Equipos de computo

Red Wifi

Impresoras conectadas

Operaciones remotas

Dispositivos utilizados

Red Wifi domestica

Proceso de manejo de información

Manejo de información interna de los procesos

Documentación administrativa y comercial

Información sensible sobre clientes y proveedores

Cumplimiento normativo

Identificación de requerimientos legales (protección de datos personales)

Conocer estándares y políticas de seguridad existentes

Análisis del personal

Estrategia de Trabajo

Se realiza el levantamiento de información por medio de entrevistas, llamadas y revisión de documentos.

Indagación física de los activos tecnológicos

Evaluación técnica de los dispositivos y redes utilizados en la oficina y de forma remota

Análisis de las brechas de seguridad en base a la norma ISO/IEC 27001 y Magerit.

Entregables

Inventario de activos tecnológicos de información de la compañía

Evaluación de riesgos y vulnerabilidades

Informe diagnostico con recomendaciones

Responsables de la Gestión de los Activos

Se realiza la definición y la asignación de roles y responsabilidades para la gestión de activos de la compañía en base al levantamiento de información.

Tabla 1

Activo de Información

Nombre activo	Descripción	Responsable
Computadores	Computadores asignados a los empleados de la empresa.	Todos los empleados
Impresora	Impresora asignada al uso de la compañía.	Todos los empleados
Teclados	Periférico designado a cada computador.	Todos los empleados
Mouse	Periférico designado a cada computador.	Todos los empleados
Pantallas	Pantallas que pueden ser utilizadas como complemento de trabajo.	Todos los empleados
Office 365	Licencia de herramienta ofimática.	Gerente
Dominios	Dominios para los correos electrónicos de la empresa.	Gerente
Antivirus ESET	Licencia de software utilizado para la protección de la información a nivel local y red.	Gerente
Documentos físicos	Documentación física que se encuentra almacenada como archivo.	Gerente - Todos los empleados
Empleados	Personal los cuales realizan diferentes labores para el funcionamiento de la compañía.	Gerente
Cámaras	Cámara utilizada para monitorear la actividad de la oficina principal.	Gerente
Celulares	Celulares que se utilizan para el proceso interno de la compañía.	Gerente - Todos los empleados
Mega	Repositorio de información de la compañía.	Gerente - Todos los empleados
Red Wifi	Internet wifi que se usa en la oficina	Gerente

Nombre activo	Descripción	Responsable
	principal.	
Contraseñas	Gestión de las contraseñas y credenciales de acceso.	Gerente - Todos los empleados
Hojas de vida de empleados	Archivo Físico con la información de los empleados de la organización.	Gerente

Nota. Activos de información de la compañía.

Valoración Inicial

Dado que la empresa no cuenta con ningún control de seguridad establecidos, se presenta a continuación los puntos que permiten identificar aspectos relevantes del análisis de riesgos y el cumplimiento normativo.

Análisis de Riesgos. En análisis realizado por medio de la metodología Magerit permitió identificar las amenazas internas y externas que afectan los activos de la compañía.

Amenazas Externas. Las amenazas externas se relacionan a los ciberataques, la interrupción de servicio, la suplantación de identidad y los errores de mantenimiento o actualizaciones.

Ciberataques. Se presentan por la fuga de información en activos como contraseñas, software como mega y el office 365.

Interrupción de Servicio. La interrupción de un servicio puede presentarse por el corte en el suministro eléctrico, los errores de configuración DNS.

Suplantación de identidad: Existe riesgos de suplantación de identidad cuando se hace uso de la aplicación Mega, donde el atacante puede obtener acceso a información sensible.

Errores en mantenimiento o actualización: Este tipo de amenaza se presenta en activos de

software o hardware los cuales pueden ser susceptibles a fallos en las actualizaciones los cuales abren brechas de seguridad.

Amenazas Internas. Las amenazas internas se relacionan a los errores humanos, en las malas prácticas de gestión de accesos, en la fuga de información accidental o intencional.

Errores Humanos. Los errores humanos se presentan por el manejo inadecuado de contraseñas, donde la generación de contraseñas débiles o incluso su almacenamiento inseguro puede facilitar los accesos no autorizados.

Prácticas inadecuadas de gestión de accesos: En aplicaciones como el antivirus se realiza segmentación insuficiente de roles que pueden permitir acciones indebidas.

Fuga de Información Accidental o Intencional. La fuga de información accidental o intencional se puede presentar por el manejo descuidado de documentos por parte de los empleados y la falta de controles.

Se pudo establecer que los activos de información con una criticidad alta son contraseñas (valor del riesgo 24-25), mega (valor del riesgo 19), red Wifi (valor del riesgo 19).

En la valoración de los activos críticos, se encontró que aquellos con mayor criticidad con las contraseñas (Valoración de riesgo 24-25), la aplicación mega (Valoración de riesgo 19) y la red Wifi (Valoración de riesgo 19). Con lo anterior las medidas que se deben priorizar será la gestión de credenciales, control de información en la nube y el fortalecimiento de políticas a nivel de la red.

Se puede evidenciar una carencia de seguridad informática de la compañía, lo cual no solo incrementa la probabilidad de ataques, sino que capacidad de respuesta está limitada.

Adicional, se visualiza un incumplimiento legal al no cumplir con las normativas legales como la ley 1581 de 2012 la cual establece normas generales sobre la protección de datos.

Análisis Técnico de Seguridad

Inventario de Controles

Tabla 2

Inventario de Controles Existentes

Control técnico	Descripción	Acciones/recomendaciones
Red-Wifi	Red wifi configurada con protocolo WPA3, se encuentra protegida con una contraseña y no se encuentra abierta.	El cambio de contraseña debe realizarse periódicamente.
Antivirus ESET	Configurada con escaneo, actualización de amenazas y detección de amenazas.	Las definiciones y actualizaciones deben realizarse de forma automática.
Sistema de detección IDS/IPS	No se encuentra implementado actualmente.	Se recomienda la implementación de un IDS/IPS para monitorear y prevenir intrusiones a nivel de red.
Segmentación de red	No se encuentra segmentada a red.	Se recomienda la segmentación de la red.
Procedimientos de red	Procedimientos de red para la conexión de dispositivos a la red Wifi.	Se debe establecer políticas de conexión de dispositivos, gestión de contraseñas y control de acceso.

Nota. Inventario de los controles existentes para la compañía.

Referente al inventario de controles se evidencia que la compañía cuenta con medidas muy básicas como la protección WPA3 en la Wifi y su antivirus. Sin embargo, la falta de un sistema IDS/IPS y la carencia de una red fragmentada hacen que la compañía se vea incapacitada para una respuesta oportuna a incidentes de seguridad.

Las brechas de seguridad analizadas muestran que los controles implementados son insuficientes en relación a la norma ISO 27001, la cual hace relevancia en los controles

preventivos y monitoreo.

Análisis de Riesgos

El análisis de los riesgos ha realizado utilizando la norma ISO 27001 y la metodología Magerit, donde se realizó la identificación de los activos, las amenazas-vulnerabilidades, la valoración cuantitativa y cualitativa de los activos, su evaluación y tratamiento.

Identificación de Amenazas y Vulnerabilidades. Seguido se presenta la identificación de las amenazas y vulnerabilidades relacionadas a los activos de información.

Tabla 3

Amenazas Vulnerabilidades

Activos de Información	Nombre del activo	Valoración del Riesgo	Amenazas Metodología Magerit	Vulnerabilidades
Hardware	Computadores	13	[I6] Corte del suministro eléctrico	Se interrumpe el uso del PC por subministro eléctrico.
Hardware	Computadores	19	[A6] Abuso de privilegios de acceso	Falta de segmentación de roles al no establecer perfiles de usuario según las necesidades laborales.
Hardware	Computadores	9	[I5] Avería de origen físico o lógico	Fallo en el sistema que puede ser provocado por problemas técnicos, desastres naturaleza o errores humanos.
Hardware	Impresora	9	[I5] Avería de origen físico o lógico	La falta de mantenimiento preventivo puede ocasionar falla de origen físico, y la falta de monitoreo de errores en la omisión de alertas puede ocasionar fallos de tipo lógico.
Hardware	Impresora	9	[I3] Contaminación mecánica	Agentes externos como el polvo, residuos, tinta,

Activos de Información	Nombre del activo	Valoración del Riesgo	Amenazas Metodología Magerit	Vulnerabilidades
				etc. Afecta los componentes mecánicos, reduciendo su funcionalidad o provocando fallos.
Hardware	Teclados	9	[N2] Daños por agua	Puede ser causados por derrame de líquidos, humedad excesiva o exposición a condiciones climáticas inadecuadas.
Hardware	Mouse	9	[N2] Daños por agua	Puede ser causados por derrame de líquidos, humedad excesiva o exposición a condiciones climáticas inadecuadas.
Software	Office 365	15	[E20] Vulnerabilidades de los programas (software)	Debilidades en el desarrollo, configuración o mantenimiento del software que pueden ser explotadas por un atacante.
Software	Office 365	15	[E21] Errores de mantenimiento / actualización de programas (software)	Fallos o deficiencias durante las actualizaciones, parches o configuraciones del sistema.

Activos de Información	Nombre del activo	Valoración del Riesgo	Amenazas Metodología Magerit	Vulnerabilidades
Servicios	Dominios	14	[E19] Fugas de información	Exposición no autorizada de datos sensibles por medio del uso o la gestión de sistemas de correos electrónicos.
Servicios	Dominios	9	[A24] Denegación de servicio	La negación de servicios puede presentarse por la configuración incorrecta del DNS, el DNS no tiene implementado límites de solicitudes, se carece de filtro de tráfico, etc.
Software	Antivirus ESET	12	[E20] Vulnerabilidades de los programas (software)	Se pueden exponer sistemas a diferentes amenazas por medio de la ejecución de código remoto, por medio del motor de análisis de archivos, por falta de actualización y parches, etc.
Software	Antivirus ESET	13	[A6] Abuso de privilegios de acceso	Un usuario autorizado o un atacante externo obtiene permisos elevados o

Activos de Información	Nombre del activo	Valoración del Riesgo	Amenazas Metodología Magerit	Vulnerabilidades
				configuraciones críticas con el fin de desactivarlo, modificarlo o realizar alguna explotación.
Datos	Documentos físicos	14	[E18] Destrucción de información	Se puede presentar la perdida, daño o eliminación intencional de datos valiosos.
Datos	Documentos físicos	12	[A15] Modificación deliberada de la información	Se presenta alteración física, falsificación o manipulación de documentos, con fines maliciosos.
Personal	Empleados	15	[E19] Fugas de información	La información confidencial puede ser divulgada, robada o filtrada por empleados. Puede presentarse de manera intencional o accidental.
Personal	Empleados	12	[E28] Indisponibilidad del personal	La información confidencial puede ser divulgada, robada o filtrada por empleados. Puede presentarse de

Activos de Información	Nombre del activo	Valoración del Riesgo	Amenazas Metodología Magerit	Vulnerabilidades
				manera intencional o accidental.
Hardware	Cámaras	9	[I3] Contaminación mecánica	Agentes externos como el polvo, residuos etc. Afecta los componentes mecánicos, reduciendo su funcionalidad o provocando fallos.
Hardware	Cámaras	9	[I6] Corte del suministro eléctrico	Se interrumpe la vigilancia y la capacidad de monitorear posibles incidentes o eventos de seguridad.
Hardware	Celulares	13	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Los riesgos surgen cuando se cometen errores en el mantenimiento o la actualización del dispositivo móvil, lo que puede afectar su funcionamiento, seguridad o integridad.
Hardware	Celulares	15	[A11] Acceso no autorizado	Personal no autorizado accede, modifica o roba información del dispositivo móvil,

Activos de Información	Nombre del activo	Valoración del Riesgo	Amenazas Metodología Magerit	Vulnerabilidades
				comprometiendo la privacidad, seguridad de los datos y la integridad del dispositivo.
Datos	Mega	15	[E19] Fugas de información	La información sensible se puede filtrar o puede ser accedida por personas no autorizadas.
Datos	Mega	19	[A5] Suplantación de la identidad del usuario	Un atacante puede acceder a una cuenta legitima de un usuario para robar, modificar o eliminar datos.
Comunicaciones	Red Wifi	9	[I8] Fallo de servicios de comunicaciones	Interrupción o falla del servicio de red inalámbrica, lo cual puede afectar los procesos de la compañía.
Comunicaciones	Red Wifi	19	[A11] Acceso no autorizado	Personal no autorizado se conecta a la red wifi, aprovechando la debilidad en las configuraciones y contraseñas.
Datos	Contraseñas	25	[A11] Acceso no autorizado	El acceso no autorizado referente a las

Activos de Información	Nombre del activo	Valoración del Riesgo	Amenazas Metodología Magerit	Vulnerabilidades
				contraseñas se presenta con la generación de contraseñas débiles, reutilización de contraseñas, almacenamiento inseguro, etc.
Datos	Contraseñas	24	[E19] Fugas de información	La fuga de información por las contraseñas se presenta por el no uso de contraseñas en los pc, por su almacenamiento inseguro, errores humanos, etc.
Datos	Hojas de vida de empleados	9	[E18] Destrucción de información	Se pueden presentar vulnerabilidades que implican la pérdida o daño de los datos, causado de manera accidental o mal intencionada.
Hardware	Pantallas	9	[N2] Daños por agua	Puede ser causados por derrame de líquidos, humedad excesiva o exposición a condiciones climáticas inadecuadas.

Nota. Amenazas y vulnerabilidades que se presentan en los diferentes activos de información.

El análisis de las amenazas y vulnerabilidades muestra que los activos más críticos son las contraseñas (Valor del riesgo 25), aplicación mega y red Wiffi (Valor del riesgo 19). Esto muestra que los activos más débiles son aquellos de gestión de accesos, servicios a nivel de la nube y comunicaciones, esto refuerza la necesidad de las políticas de seguridad y la capacitación de personal.

Así mismo la presencia de fugas de información que se evidencian como amenazas en activos como empleados, documentos físicos y plataformas en la nube muestra la inexistencia de políticas de seguridad de la información y los protocolos de seguridad de los datos. El objetivo de diseñar políticas basadas en la ISO 27000 será de gran valor para contrarrestar las amenazas y vulnerabilidades que presenta la compañía.

Áreas Vulnerables. Seguido se presentan las áreas vulnerables según lo identificado en las amenazas y vulnerabilidades.

Tabla 4

Áreas vulnerables

Área	Vulnerabilidades	Acciones/recomendaciones
Hardware	Cortes eléctrico	Generar planes de mantenimiento
	Daños por agua	preventivo.
	Contaminación mecánica	
	Errores de mantenimiento	
Software	Vulnerabilidades en programas	Gestión de actualización
	Errores de mantenimiento	Configuración adecuada de herramientas
Datos	Fuga de información	Generar copias de seguridad periódicas
	Destrucción de datos	Definir políticas de acceso
	Modificación maliciosa	
Comunicaciones	Red Wifi no segmentada	Segmentación de la red
	Configuración insegura de red	
Personal	Fugas de información por causa de	Concientización y formación sobre la
	errores humanos.	seguridad de la información.

Nota. Estas son las áreas vulnerables de la organización según el análisis realizado a los activos de información.

En análisis de las áreas vulnerables, el hardware muestra vulnerabilidades de cortes eléctricos, daños por fuga y contaminación mecánica los cuales pueden ser tratados con un plan de mantenimiento preventivo.

Un punto de acceso importante de vulnerabilidades se encuentra la Wifi la cual no se encuentra segmentada y posee una configuración insegura, lo cual presenta una brecha de seguridad activa y de alto riesgo, señalando la necesidad de implementar controles de

segmentación y gestión de accesos en relación con la ISO 27000.

En cuanto al área de datos las amenazas de fugas de información, la destrucción de daos y la modificación maliciosa, muestran carencia de políticas de acceso y las copias de seguridad.

El área personal, muestra la vulnerabilidad como fugas de información por causa de errores humanos los cuales serán solucionados si se realiza la concientización y formación de seguridad de la información en sus empleados, lo cual será generado mediante el plan de formación de seguridad.

Evaluación de Controles Existentes-Inexistentes. La evaluación de controles que se presentan a continuación evidencia la crítica situación de la compañía ya que no cuenta con ningún control existente.

Tabla 5

Controles

Activos de Información	Nombre del activo	Control	Tipo - ISO 27001:2022	Control - ISO 27001:2022	Tipo control	Estado
	Computadores	No existe un plan de mantenimiento preventivo y/o programado para el suministro eléctrico.	Control_Organizacional	seguridad de la información durante una interrupción	Preventivo	Inexistente
Hardware	Computadores	No existe una política especifica y establecida que trate sobre el manejo del abuso de privilegios en los computadores.	Control_Tecnológico	Derechos de acceso privilegiados	Preventivo	Inexistente
Hardware	Computadores	No existe una política especifica y establecida que trate sobre el manejo de averías de origen físico y lógico.	Control_Físico	Protección contra amenazas físicas y medioambientales	Preventivo	Inexistente
Hardware	Impresora	No existe una política especifica y establecida que trate sobre el manejo de averías de origen físico y lógico.	Control_Físico	Protección contra amenazas físicas y medioambientales	Preventivo	Inexistente

Activos de Información	Nombre del activo	Control	Tipo - ISO 27001:2022	Control - ISO 27001:2022	Tipo control	Estado
Hardware	Impresora	No existe una política especifica y establecida que trate sobre el manejo de la contaminación mecánica	Control_Físico	Mantenimiento de equipos	Preventivo	Inexistente
Hardware	Teclados	No existe una política especifica y establecida que trate sobre el manejo de daños ocasionados por el agua	Control_Físico	Protección contra amenazas físicas y medioambientales	Preventivo	Inexistente
Hardware	Mouse	No existe un plan de mantenimiento preventivo y/o programado a la red de la organización.	Control_Físico	Protección contra amenazas físicas y medioambientales	Preventivo	Inexistente
Software	Office 365	No existe una política de seguridad para las vulnerabilidades de los programas de Software	Control_Tecnológico	Gestión de las vulnerabilidades técnicas	Preventivo	Inexistente
Software	Office 365	No existe una política de seguridad para las vulnerabilidades de los errores de	Control_Tecnológico	Gestión de las vulnerabilidades técnicas	Preventivo	Inexistente

Activos de Información	Nombre del activo	Control	Tipo - ISO 27001:2022	Control - ISO 27001:2022	Tipo control	Estado
		mantenimiento/actualización de programas				
Servicios	Dominios	No existe una política de seguridad para la fuga de información en los servicios de dominio	Control_Tecnológico	Prevención de fuga de datos	Preventivo	Inexistente
Servicios	Dominios	No existe una política de seguridad para la denegación de servicio en los servicios de dominio	Control_Tecnológico	Gestión de la configuración	Preventivo	Inexistente
Software	Antivirus ESET	No existe una política de seguridad para las vulnerabilidades de los programas de Software	Control_Tecnológico	Gestión de las vulnerabilidades técnicas	Preventivo	Inexistente
Software	Antivirus ESET	No existe una política especifica y establecida que trate sobre el manejo del abuso de privilegios en los antivirus.	Control_Tecnológico	Derechos de acceso privilegiados	Preventivo	Inexistente
Datos	Documentos físicos	No está establecido el procedimiento para realizar el back-up	Control_Tecnológico	Copias de seguridad de la información	Preventivo	Inexistente

Activos de Información	Nombre del activo	Control	Tipo - ISO 27001:2022	Control - ISO 27001:2022	Tipo control	Estado
		para la información.				
Datos	Documentos físicos	No está establecido el procedimiento para la modificación deliberada de información.	Control_Físico	Protección contra amenazas físicas y medioambientales	Preventivo	Inexistente
Personal	Empleados	No existen políticas de seguridad para la fuga de información.	Control_Personal	Acuerdos de confidencialidad o no divulgación	Preventivo	Inexistente
Personal	Empleados	No existen políticas de seguridad para la indisponibilidad de personal.	Control_Personal	Condiciones del empleo	Preventivo	Inexistente
Hardware	Cámaras	No existe una política especifica y establecida que trate sobre el manejo de la contaminación mecánica	Control_Físico	Mantenimiento de equipos	Preventivo	Inexistente
Hardware	Cámaras	No existe un plan de mantenimiento preventivo y/o programado para el suministro eléctrico	Control_Organizacional	seguridad de la información durante una interrupción	Preventivo	Inexistente

Activos de Información	Nombre del activo	Control	Tipo - ISO 27001:2022	Control - ISO 27001:2022	Tipo control	Estado
Hardware	Celulares	No existe una política de seguridad para las vulnerabilidades de los errores de mantenimiento/actualización de programas	Control_Tecnológico	Gestión de las vulnerabilidades técnicas	Preventivo	Inexistente
Hardware	Celulares	No existen políticas para el manejo del acceso no autorizado.	Control_Tecnológico	Restricción de acceso a la información	Preventivo	Inexistente
Datos	Mega	No existen políticas de seguridad para la fuga de información.	Control_Tecnológico	Prevención de fuga de datos	Preventivo	Inexistente
Datos	Mega	No existen políticas de seguridad referente a la suplantación de identidad.	Control_Tecnológico	Requisitos de seguridad en aplicaciones	Preventivo	Inexistente
Comunicaciones	Red Wifi	No existen políticas de seguridad referente al fallo de servicios de comunicación con la Wifi.	Control_Tecnológico	Restricción de acceso a la información	Preventivo	Inexistente
Comunicaciones	Red Wifi	No existen políticas para el manejo del acceso no autorizado.	Control_Tecnológico	Restricción de acceso a la información	Preventivo	Inexistente

Activos de Información	Nombre del activo	Control	Tipo - ISO 27001:2022	Control - ISO 27001:2022	Tipo control	Estado
Datos	Contraseñas	No existen políticas para el manejo del acceso no autorizado.	Control_Tecnológico	Restricción de acceso a la información	Preventivo	Inexistente
Datos	Contraseñas	No existen políticas de seguridad para la fuga de información.	Control_Tecnológico	Prevención de fuga de datos	Preventivo	Inexistente
Datos	Hojas de vida de empleados	No existe una política especifica y establecida que trate sobre el manejo de la documentación en físico usada por la organización.	Control_Físico	Protección contra amenazas físicas y medioambientales	Preventivo	Inexistente
Hardware	Pantallas	No existe una política especifica y establecida que trate sobre el manejo de daños ocasionados por el agua	Control_Físico	Protección contra amenazas físicas y medioambientales	Preventivo	Inexistente

Nota. Controles existentes e inexistentes de la compañía en sus activos de información.

El análisis de controles muestra la carencia de un marco de seguridad establecidos por la compañía. Algunos de los controles que están alineados con la ISO 27000 se encuentran en estado inexistente mostrando una brecha en la gestión de la información comprometiendo los activos de la compañía.

Los pilares de la información que son la confidencialidad, integralidad y disponibilidad, se ven claramente afectados por la inexistencia de mecanismos como las políticas de gestión de accesos, procedimientos de respaldo de información entre otros.

Fortalecer la cultura de la seguridad en la compañía se hace cada vez más necesaria ya que la ausencia de protocolos en la actuación del personal y la gestión de la información interna muestra los riesgos en los factores externos o tecnológicos, pero aún más en los errores humanos y sus prácticas inseguras. A New Age of Cybersegurity Culture, estudio de KPMG Colombia en enero del 2025, identifica que los errores humanos siguen siendo uno de los principales desafíos para las organizaciones. (*A New Age of Cybersecurity Culture - KPMG Colombia*, 2025)

La prioridad del desarrollo del plan director de seguridad deberá centrarse también la implementación de controles técnicos, pero también en la priorización de políticas que se adapten a la realidad actual de la compañía, con el fin de reducir las brechas de seguridad encontradas.

Se debe priorizar algunos controles debido al impacto que representan:

Contraseñas (Valor 25): Se requiere de forma urgente establecer políticas con el fin de restringir acceso no autorizado y prevención de fugas de información.

Mega (Valor 19): Establecer políticas con el fin de evitar suplantación de identidad y fugas de datos.

Red Wifi (Valor 19): Generar políticas contra accesos no autorizados.

Computadores (Valor 19): Se requiere de políticas de seguridad que permita controlar los privilegios elevados que poseen los usuarios.

Tratamiento del Riesgo. El tratamiento del riesgo se realiza en base al análisis realizado a los activos de información de la compañía, en la búsqueda de garantizar la confidencialidad,

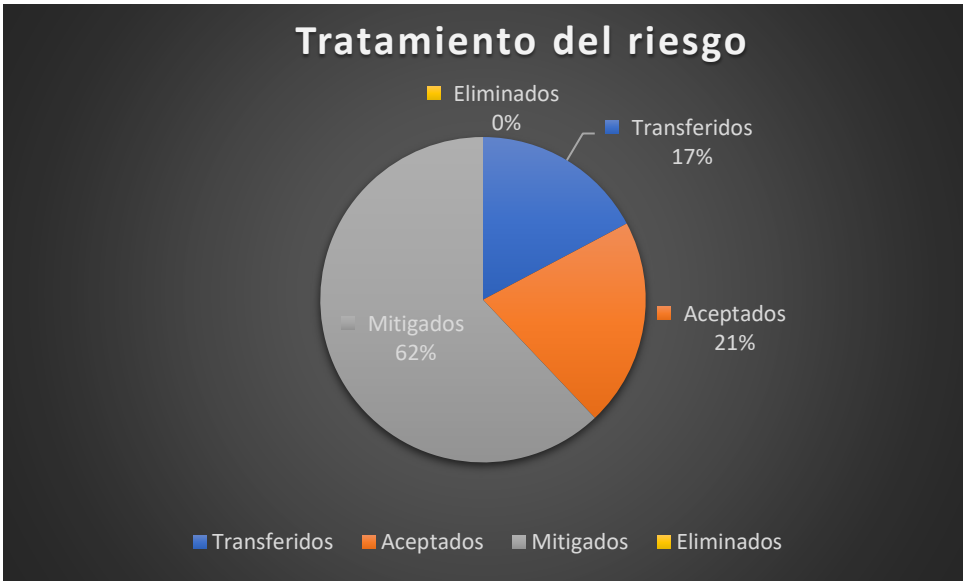
integridad y disponibilidad. Con la identificación de amenazas y vulnerabilidades, se han definido tratamientos que permiten minimizar el impacto y la ocurrencia de incidentes.

Se adoptan las opciones del tratamiento del riesgo recomendadas por la metodología Magerit y la ISO 27000, trasferir, mitigar, aceptar o eliminar los riesgos. El tratamiento del riesgo se alinea con la estrategia corporativa, estableciendo medidas de protección a sus activos.

En la siguiente grafica se evidencia como se determinó el tratamiento de los riesgos para los activos, según el análisis realizado.

Figura 3

Tratamiento del Riesgo



Nota. Imagen propia, diseñada con datos del análisis de los riesgos.

Riesgos Transferidos. Los activos transferidos delegan la responsabilidad de proteger y gestionarlos, resulta más eficiente transferir el riesgo a un tercero que asumirlo, ya que es posible que muchos de estos riesgos estén implícitos en aplicaciones que son ajenas al control total de la compañía.

Con la transferencia de estos riesgos se reduce gastos financieros y operativos de la compañía, asegurando que un tercero asuma la responsabilidad en caso de materializarse el incidente.

Tabla 6

Riesgos Transferidos

Activos de Información	Nombre del activo	Control	Nivel de aceptación	Descripción del control
Software	Office 365	Gestión de las vulnerabilidades técnicas	I	NA
Hardware	Office 365	Gestión de las vulnerabilidades técnicas	I	NA
Servicio	Dominios	Prevención de fuga de datos	M	NA
Servicio	Dominios	Gestión de la configuración	M	NA
Software	Antivirus	Gestión de las vulnerabilidades técnicas	M	NA
Hardware	Celulares	Gestión de las vulnerabilidades técnicas	M	NA

Nota. Activos que son transferidos ya que no pueden ser controlados internamente por la organización sino por terceros.

Riesgos Aceptados. Sobre los siguientes activos no se implementarán medidas ya que se considera que el riesgo es tolerable. Se asume conscientemente que estos riesgos se materialicen ya que los controles pueden llegar a ser más costoso que su propio beneficio.

Tabla 7

Riesgos Aceptados

Activos de Información	Nombre del activo	Control	Nivel de aceptación
Hardware	Teclado	Gestión de las vulnerabilidades técnicas	M
Hardware	Mouse	Protección contra amenazas físicas y medioambientales	M
Personal	Empleados	Proceso disciplinario	M
Hardware	Cámaras	seguridad de la información durante una interrupción	M
Comunicaciones	Red Wifi	Restricción de acceso a la información	M
Hardware	Pantallas	Protección contra amenazas físicas y medioambientales	A

Nota. Activos aceptados los cuales no requieren un tratamiento ya que su riesgo es tolerable.

Riesgo Residual y Aceptación. El análisis del riesgo según la metodología Magerit no concluye con la identificación de amenazas y la aplicación de controles, sino que contempla el riesgo residual el cual es el nivel de riesgo que permanece aún después de implementar medidas de seguridad, preventivas y correctivas. En la actualidad la compañía no cuenta con controles implementados para sus activos, sin embargo, en el análisis realizado se definieron controles recomendados para cada activo, con lo cual se proyecta un nivel de riesgo residual tolerable. (coordinación de contenidos et al., 2012)

La aceptación de estos riesgos se fundamenta en lo siguiente:

- El riesgo residual se encuentra dentro de los umbrales de tolerancia.

- La implementación de controles adicionales, podrían generar costos, complejidad o impactos operativos.
- La materialización de estos riesgos, no comprometen de manera significativa los objetivos de la seguridad de la información de la compañía.
- La priorización de la inversión en seguridad se orienta hacia los activos y amenazas de mayor impacto.

Justificación de Aceptación de Riesgos por Activo

Tabla 8

Justificación Riesgos Aceptados

Activos de Información	Nivel de riesgo	Controles propuestos	Justificación
Teclado	Medio	Gestión de las vulnerabilidades técnicas	Es un activo fácilmente reemplazable, el impacto de un incidente es bajo. El riesgo se acepta en tanto se gestionan los activos más críticos.
Mouse	Medio	Protección contra amenazas físicas y medioambientales	Es un activo fácilmente reemplazable, el impacto de un incidente es bajo. El riesgo se acepta de manera consistente debido a su baja criticidad.
Empleados	Medio	Proceso disciplinario	El riesgo humano es gestionado por políticas de seguridad y el plan de formación y capacitación. El riesgo se acepta en tanto se formalicen los procesos y las políticas.
Cámaras	Medio	Mantenimiento preventivo de equipos	Aunque no se cuenta con controles, su impacto en la seguridad es complementario. Se acepta el riesgo hasta que se priorice su implementación.
Red Wifi	Medio	Autenticación segura y monitoreo de disponibilidad	El riesgo identificado corresponde a la indisponibilidad del servicio por fallas técnicas o interrupciones. El riesgo residual se considera tolerable ya que no compromete de manera inmediata la

Activos de Información	Nivel de riesgo	Controles propuestos	Justificación
			continuidad de los procesos.
Pantallas	Bajo	Protección contra amenazas físicas y medioambientales	El riesgo se acepta por su baja criticidad.

Nota. Justificación de riesgos aceptados, los cuales no requieren un tratamiento ya que su riesgo es tolerable.

La aceptación de los riesgos descritos anteriormente, se presentan teniendo en cuenta que la organización aun no cuenta con controles implementados para estos activos de información. La aceptación de estos riesgos, se generan de manera temporal y estratégica, permitiendo priorizar recursos hacia los activos que se encuentran en un mayor riesgo.

Los riesgos que presentan estos activos, aunque no comprometen la continuidad de los procesos de negocio de la compañía, no implica que estos sean desestimados, sino que hacen parte de los riesgos que la compañía deberá ir incluyendo progresivamente para la generación de controles, conforme a disponibilidad de recursos y los lineamientos por parte de la gerencia.

Riesgos Mitigados. Sobre los siguientes activos se implementarán medidas y controles con el fin de reducir la probabilidad de que ocurra el riesgo. En estos activos se considera mantener un control directo, donde se han adoptado medidas de mitigación. La mitigación de los riesgos disminuye la probabilidad o el impacto de la materialización del riesgo por medio de la implementación de controles.

Tabla 9

Riesgos Mitigados

Activos de Información	Nombre del activo	Control	Nivel de aceptación	Descripción del control
Hardware	Computadores	Derechos de acceso privilegiados	I	Establecer la implementación de controles administrativos como la definición y documentación de roles y perfiles de acceso, políticas de gestión de cuentas y la capacitación de persona.
Hardware	Computadores	Seguridad de la información durante una interrupción	M	Se recomienda la instalación de UPS que permiten mantener los pc con energía hasta guardar completamente la información. Generar controles y capacitaciones ante fallas eléctricas.
Hardware	Computadores	Protección contra amenazas físicas y medioambientales	M	Se recomienda controles como mantenimiento preventivo del Hardware, actualización y parches de seguridad, condiciones ambientales adecuadas y políticas de renovación tecnológica.
Hardware	Impresora	Protección contra amenazas físicas y medioambientales	M	Se recomienda controles como mantenimiento preventivo del Hardware, actualización y parches de seguridad, condiciones ambientales adecuadas y políticas

Activos de Información	Nombre del activo	Control	Nivel de aceptación	Descripción del control
				de renovación tecnológica.
Hardware	Impresora	Mantenimiento de equipos	M	Se recomienda controles como mantenimiento preventivo del Hardware, actualización y parches de seguridad, condiciones ambientales adecuadas y políticas de renovación tecnológica.
Software	Antivirus ESET	Derechos de acceso privilegiados	I	Establecer la implementación de controles como la gestión de accesos y privilegios, capacitación de usuarios, protección de contraseñas para antivirus, bloqueo de permisos administrativos y el monitoreo de integralidad del antivirus.
Datos	Documentos físicos	Copias de seguridad de la información	M	Digitalización y almacenamiento seguro de los documentos críticos junto a medidas físicas de protección contra incendios, inundaciones. Etc.
Datos	Documentos físicos	Restricción de acceso a la información	M	Implementación de políticas de control de acceso y custodia de documentos físicos.
Hardware	Cámaras	Mantenimiento de	M	Se recomienda controles como

Activos de Información	Nombre del activo	Control	Nivel de aceptación	Descripción del control
		equipos		mantenimiento preventivo del Hardware, actualización y parches de seguridad, condiciones ambientales adecuadas y políticas de renovación tecnológica.
Hardware	Celulares	Gestión de las vulnerabilidades técnicas	M	Establecer políticas del uso y mantenimiento de dispositivos móviles, capacitación del personal sobre las buenas prácticas del manejo de estos dispositivos, establecer actualizaciones programadas y realizar auditorías periódicas a los dispositivos.
Personal	Empleados	Acuerdos de confidencialidad o no divulgación	I	Generar políticas de seguridad de la información como el manejo de la información confidencial y como debe de protegerse.
Hardware	Celulares	Restricción de acceso a la información	I	Establecer políticas del uso y mantenimiento de dispositivos móviles, capacitación del personal sobre las buenas prácticas del manejo de estos dispositivos, establecer actualizaciones programadas y realizar auditorías periódicas a los dispositivos.

Activos de Información	Nombre del activo	Control	Nivel de aceptación	Descripción del control
Software	Mega	Prevención de fuga de datos	I	Establecer políticas sobre el uso de servicios en la nube, acuerdos de confidencialidad, capacitación de personal, gestionar los accesos, activar un MFA, los dispositivos deben ser seguros.
Software	Mega	Requisitos de seguridad en aplicaciones	I	Establecer políticas sobre el uso de servicios en la nube, acuerdos de confidencialidad, capacitación de personal, gestionar los accesos, activar un MFA, los dispositivos deben ser seguros.
Comunicaciones	Red Wifi	Restricción de acceso a la información	I	Establecer políticas para el uso de la red, contraseñas fuertes, capacitación de personal, control de accesos.
Personal	Contraseñas	Restricción de acceso a la información	I	Generar políticas de seguridad sobre las contraseñas donde se establezca la longitud y complejidad, la reutilización y la frecuencia para el cambio. Capacitación de usuarios.
Hardware	Contraseñas	Prevención de fuga de datos	I	Generar políticas de seguridad sobre las contraseñas donde se establezca la longitud y complejidad, la reutilización y la

Activos de Información	Nombre del activo	Control	Nivel de aceptación	Descripción del control
				frecuencia para el cambio. Capacitación de usuarios.
Datos	Hojas de vida de empleados	Protección contra amenazas físicas y medioambientales	M	Digitalización y almacenamiento seguro de los documentos críticos junto a medidas físicas de protección contra incendios, inundaciones. Etc.

Nota. Sobre estos activos se implementarán medidas y controles.

El tratamiento del riesgo se plantea con el control a aplicar según la norma ISO27001, transfiriendo, aceptando, eliminando o mitigándolo.

El control directo de la protección de los servicios como Office 365, dominios y antivirus de la compañía, no es posible ya que dependen de terceros lo cual hace que sean transferidos.

Aunque algunos riesgos son aceptables, no comprometen la continuidad del negocio por esta razón la compañía no justifica inversiones significativas en controles adicionales, es de vital importancia entender que los riesgos aceptables no indican que se ignoran completamente.

Los activos mitigados representan las brechas de seguridad más críticas para la organización (Contraseñas, red Wifi, servicios en la nube (Mega) y dispositivos móviles), la mitigación de estos activos, son coherentes con a la necesidad en la gestión de accesos, el uso de servicios digitales y las prácticas inadecuadas de los empleados. Esto indica la necesidad de diseñar políticas de seguridad de control de accesos, protocolos con el uso de servicios en la nube y la implementación de procesos de formación para los empleados de la compañía.

El tratamiento dado a los riesgos encontrados contribuye a reducir las brechas y construir

un sistema de protección que se encuentran alineados con la norma ISO 27000.

Análisis Costo-Beneficio. A continuación, se presenta un análisis costo-beneficio dentro del tratamiento de los riesgos con el fin de valorar la conveniencia de implementar medidas de seguridad en relación entre el costo de los controles y la reducción del riesgo. De acuerdo con la metodología Magerit, este análisis busca determinar si las inversiones en seguridad resultan justificables frente al impacto económico que tendría la materialización de las amenazas sobre los activos de información.

- Impacto estimado: El impacto estimado se realiza teniendo en cuenta los posibles factores de riesgo como indisponibilidad, manipulación indebida o compromiso en su confidencialidad, integridad o disponibilidad.
- Costo del control: Se realizo la estimación del valor de la implementación de medidas de seguridad o controles como licencias, capacitaciones, infraestructura, horas de soporte técnico entre otras.
- Riesgo inicial: Es la pérdida económica potencial si no existen controles.
- Riesgo residual: Se aplica la reducción porcentual del riesgo dependiendo de la efectividad del control.
- Beneficio esperado: Es la diferencia entre el riesgo inicial y el residual.
- Relación costo-beneficio: Es la división entre el beneficio esperado y el costo del control.

Tabla 10

Costo Beneficio

Activo/Control	Nivel	Impacto estimado	Costo control	Riesgo inicial	Eficacia control	Riesgo residual	Beneficio esperado	Costo-Beneficio
Computadores/Seguridad interrupción	I	$ 30.000.000	$ 6.000.000	$ 30.000.000	50%	$ 15.000.000	$ 15.000.000	2,5
Computadores/Accesos privilegiados	M	$ 40.000.000	$ 8.000.000	$ 40.000.000	85%	$ 6.000.000	$ 34.000.000	4,3
Computadores/Protección física y medioambientales	M	$ 28.000.000	$ 5.000.000	$ 28.000.000	50%	$ 14.000.000	$ 14.000.000	2,8
Impresora/Protección física y medioambientales	M	$ 15.000.000	$ 3.000.000	$ 15.000.000	50%	$ 7.500.000	$ 7.500.000	2,5
Impresora/Mantenimiento de equipos	M	$ 12.000.000	$ 2.000.000	$ 12.000.000	50%	$ 6.000.000	$ 6.000.000	3,0
Cámaras/Mantenimiento de equipos	I	$ 18.000.000	$ 4.000.000	$ 18.000.000	50%	$ 9.000.000	$ 9.000.000	2,3
Celulares/Gestión de vulnerabilidades	M	$ 16.000.000	$ 5.000.000	$ 16.000.000	50%	$ 8.000.000	$ 8.000.000	1,6
Celulares/Restricción de acceso	M	$ 22.000.000	$ 6.000.000	$ 22.000.000	85%	$ 3.300.000	$ 18.700.000	3,1

Activo/Control	Nivel	Impacto estimado	Costo control	Riesgo inicial	Eficacia control	Riesgo residual	Beneficio esperado	Costo-Beneficio
Antivirus ESET/Accesos privilegiados	M	$ 35.000.000	$ 10.000.000	$ 35.000.000	85%	$ 5.250.000	$ 29.750.000	3,0
Mega/Fuga de datos	M	$ 50.000.000	$ 15.000.000	$ 50.000.000	85%	$ 7.500.000	$ 42.500.000	2,8
Mega/Requisitos de seguridad	I	$ 45.000.000	$ 12.000.000	$ 45.000.000	85%	$ 6.750.000	$ 38.250.000	3,2
Empleados/Acuerdos de confidencialidad	I	$ 32.000.000	$ 3.000.000	$ 32.000.000	85%	$ 4.800.000	$ 27.200.000	9,1
Documentos físicos/Copias de seguridad	I	$ 25.000.000	$ 5.000.000	$ 25.000.000	50%	$ 12.500.000	$ 12.500.000	2,5
Documentos físicos/Restricción de accesos	I	$ 22.000.000	$ 4.000.000	$ 22.000.000	50%	$ 11.000.000	$ 11.000.000	2,8
Contraseñas/Restricción de acceso	I	$ 25.000.000	$ 2.000.000	$ 25.000.000	85%	$ 3.750.000	$ 21.250.000	10,6
Contraseñas/Prevención fuga de datos	I	$ 30.000.000	$ 5.000.000	$ 30.000.000	85%	$ 4.500.000	$ 25.500.000	5,1

Activo/Control	Nivel	Impacto estimado	Costo control	Riesgo inicial	Eficacia control	Riesgo residual	Beneficio esperado	Costo-Beneficio
Hojas de vida de empleados/Protección física y medioambientales	I	$ 20.000.000	$ 3.000.000	$ 20.000.000	50%	$ 10.000.000	$ 10.000.000	3,3
Red Wifi/Restricción de acceso	M	$ 27.000.000	$ 7.000.000	$ 27.000.000	85%	$ 4.050.000	$ 22.950.000	3,3

Nota: Se realiza costo beneficio con los riesgos mitigados.

Tabla 11

Beneficios-Justificación

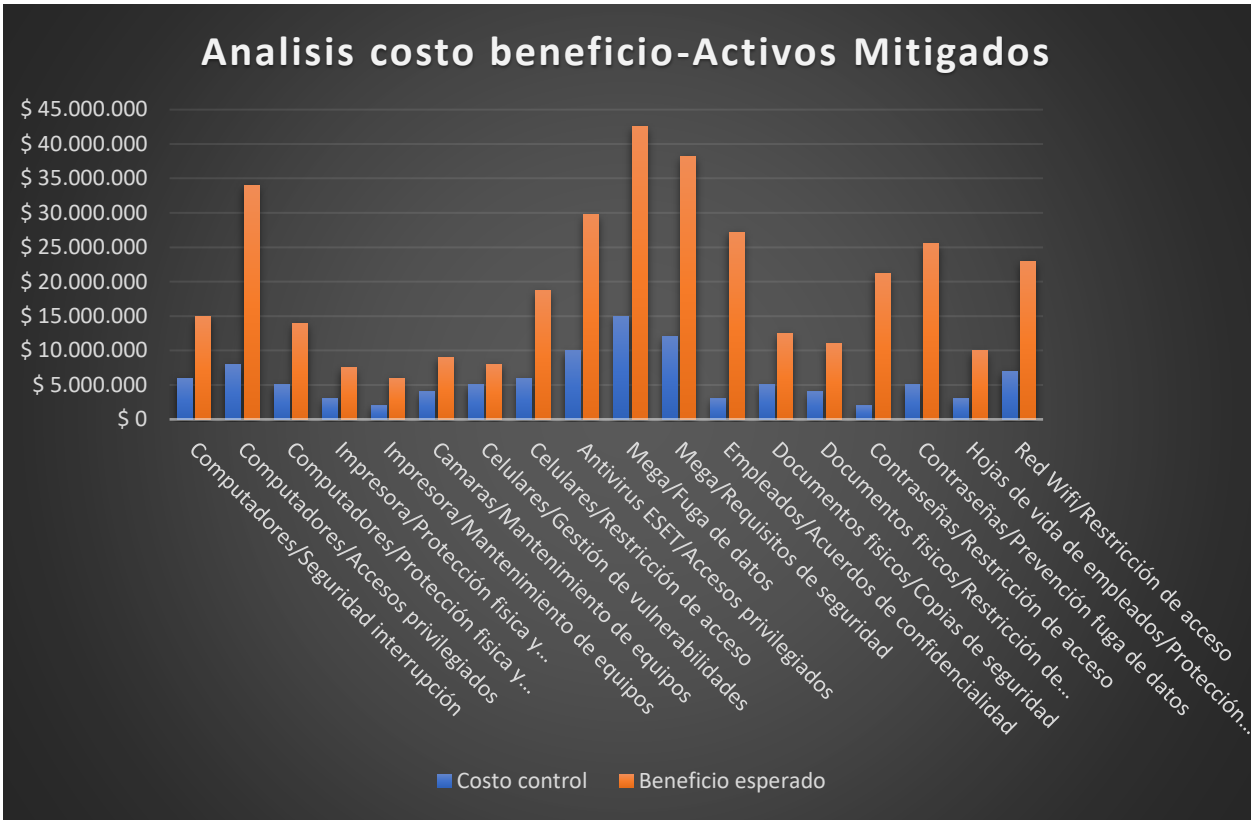
Beneficio	Justificación
	El control reduce las perdidas potenciales en 15 millones
$ 15.000.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.
	El control reduce las perdidas potenciales en 34 millones
$ 34.000.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.
	El control reduce las perdidas potenciales en 14 millones
$ 14.000.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.
	El control reduce las perdidas potenciales en 7 millones y medio
$ 7.500.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.
	El control reduce las perdidas potenciales en 6 millones
$ 6.000.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.
	El control reduce las perdidas potenciales en 9 millones
$ 9.000.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.
	El control reduce las perdidas potenciales en 8 millones
$ 8.000.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.
	El control reduce las perdidas potenciales en 18.700.000
$ 18.700.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.
	El control reduce las perdidas potenciales en 29.750.000
$ 29.750.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.
	El control reduce las perdidas potenciales en 42.500.000
$ 42.500.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.
	El control reduce las perdidas potenciales en 38.250.000
$ 38.250.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.

Beneficio	Justificación
	El control reduce las perdidas potenciales en 27.200.000
$ 27.200.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.
	El control reduce las perdidas potenciales en 12.500.000
$ 12.500.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.
	El control reduce las perdidas potenciales en 11 millones
$ 11.000.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.
	El control reduce las perdidas potenciales en 21.250.000
$ 21.250.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.
	El control reduce las perdidas potenciales en 25.500.000
$ 25.500.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.
	El control reduce las perdidas potenciales en 10 millones
$ 10.000.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.
	El control reduce las perdidas potenciales en 22.950.000
$ 22.950.000	El costo del control es mucho menor, por tal razón es conveniente implementarlo.

Nota: Beneficio y justificación de los riesgos mitigados.

Figura 4

Análisis Costo-Beneficio



Nota. Imagen propia, diseñada con datos del análisis costo-beneficio de los activos mitigados.

El análisis costo beneficio realizado indica que los controles propuestos resultan económicamente justificables y eficientes, lo anterior porque la mayoría de los activos el beneficio obtenido supera el costo del control.

Según los resultados obtenidos, las medidas de mitigación permiten reducir de forma significativa los riesgos con nivel inaceptables y moderados, alcanzando efectividad entre el 50% y 85%, lo cual genera una reducción significativa en el riesgo residual.

Los activos con mayor impacto económico muestran beneficios superiores a los $30 millones de pesos, lo cual demuestra que la inversión en seguridad es efectiva y contribuye a la

protección de la información crítica de la compañía.

Se indica que la aplicación de los controles recomendados garantiza un uso racional de los recursos de seguridad y fortalece la postura de ciberseguridad de la compañía con relación a los lineamientos de la metodología Magerit y la ISO 27000.

Recomendaciones Costo-beneficio. Se recomienda a la compañía realizar la priorización de los activos mitigados con mayor impacto y que tenga su relación costo-beneficio más favorable, como lo son computadores, red Wifi, documentos físicos entre otros, teniendo en cuenta que estos pueden generar una afectación crítica y pérdidas económicas significativas.

La implementación de los controles técnicos y administrativos de estos activos garantiza la reducción efectiva del riesgo.

Se sugiere mantener una evaluación periódica del riesgo residual y actualizar los costos de los controles anualmente, con el fin de garantizar la eficiencia y sostenibilidad de estos activos.

Viabilidad y Sostenibilidad – Riesgos Mitigados. Considerando los resultados del análisis costo-beneficio, los activos seleccionados para la mitigación, presentan una relación favorable entre el costo de implementación de los controles y el beneficio esperado en la reducción del riesgo.

Con el fin de garantizar la viabilidad y sostenibilidad de los riesgos mitigados, se propone una estrategia basada en la priorización, ejecución progresiva y la sostenibilidad operativa.

Priorización. La priorización se realiza según el impacto y rentabilidad, teniendo en cuenta los activos con mayor valor de información y que tenga mejor relación del costo-beneficio. En el caso de los controles aplicados a las contraseñas, red Wifi y acuerdos de confidencialidad, la priorización de estos activos permite optimizar los recursos disponibles y

asegura resultados inmediatos en la disminución de vulnerabilidades.

Implementación Progresiva. Se recomienda realiza la implementación progresiva por etapas:

Fase1: Controles de accesos, antivirus, gestión de contraseñas y red Wifi.

Fase 2: Controles físicos y medioambientales.

Fase 3: Gestión documental, copias de seguridad y capacitación del personal.

Sostenibilidad y Mejora Continua. Con el fin de asegurar la permanencia de los controles implementados, se recomienda:

Incluir costos de mantenimiento y actualización de software en el presupuesto anual.

Capacitación de empleados para administrar los controles implementados.

Realizar evaluaciones anuales del riesgo residual y de la eficacia de los controles implementados a los activos mitigados.

Esta estrategia permite mantener la efectividad de las medidas adoptadas, garantizando la continuidad operativa y la sostenibilidad económica del plan director de seguridad. Con esta estrategia la compañía podrá consolidar la mitigación de los riesgos críticos y avanzar hacia la gestión de la información madura y eficiente.

Evaluación del Grado de Madurez. Se realiza el grado de madurez de los controles, sobre los activos que presentan riesgos a mitigar, la evaluación del riesgo de madurez permite conocer la capacidad de la organización para gestionar los riesgos identificados y establecer un punto inicial para la mejora continua. Este grado de madurez permite identificar que tan desarrollados y documentados se encuentran los procesos de seguridad en la compañía.

Para la realización del grado de madurez se tomó como referencia el modelo de madurez propuesto por el marco COBIT 2019 el cual define niveles de madurez que son (0-

Incompleto/Inexistente, 1-Realizado, 2-Gestionado, 3-Establecido, 4-Predecible, 5-Optimizado).(Ritegno, 2018)

Con la valoración del grado de madurez, la compañía podrá tener una visión de la efectividad de sus controles actuales frente a los riesgos priorizados y de la capacidad con la que cuenta para mantener y gestionar los controles.

Tabla 12

Nivel de Madurez

Nombre-activo	Tipo de control	Control	Estado actual	Nivel de madurez COBIT	Análisis Magerit	Recomendaciones
Computadores	Organizacional	Seguridad de la información durante una interrupción	Inexistente	0-Inexistente	No existen medidas de continuidad operativa	Crear políticas de continuidad y UPS (Sistema de alimentación interrumpida)
Computadores	Tecnológico	Derechos de acceso privilegiados	Inexistente	0-Inexistente	No hay control formal sobre privilegios.	Establecer la gestión y revisión de privilegios.
Computadores	Físico	Protección contra amenazas físicas y medioambientales	Inexistente	0-Inexistente	Riesgo alto de daños físicos o ambientales.	Controles de mantenimiento preventivo y políticas de renovación tecnológica.
Impresora	Físico	Protección contra amenazas físicas y medioambientales	Inexistente	0-Inexistente	Riesgo alto de daños físicos o ambientales.	Controles y revisión ambiental.
Impresora	Físico	Mantenimiento de equipos	Inexistente	0-Inexistente	Riesgo por falta de control y mantenimiento.	Controles de mantenimiento preventivo y políticas de renovación tecnológica.

Nombre-activo	Tipo de control	Control	Estado actual	Nivel de madurez COBIT	Análisis Magerit	Recomendaciones
Antivirus ESET	Tecnológico	Derechos de acceso privilegiados	Inexistente	0-Inexistente	No se gestiona la seguridad del software.	Implementación de controles de monitoreo, actualización y políticas.
Documentos físicos	Tecnológico	Copias de seguridad de la información	Inexistente	0-Inexistente	No existe respaldo o copias de seguridad.	Digitalización y almacenamiento seguro de los documentos críticos.
Documentos físicos	Tecnológico	Restricción de acceso a la información	Inexistente	0-Inexistente	Falta de control de acceso a la información.	Implementación de políticas de control de acceso y custodia de documentos físicos.
Cámaras	Control_Personal	Acuerdos de confidencialidad o no divulgación	Inexistente	0-Inexistente	Riesgo de fallos sin control preventivo.	Se recomienda controles de mantenimiento preventivo.
Celulares	Físico	Mantenimiento de equipos	Inexistente	0-Inexistente	Riesgos por falta de controles.	Establecer políticas del uso y mantenimiento de dispositivos móviles, capacitación del personal.
Empleados	Tecnológico	Gestión de las	Inexistente	0-Inexistente	No se controla la	Generar políticas de

Nombre-activo	Tipo de control	Control	Estado actual	Nivel de madurez COBIT	Análisis Magerit	Recomendaciones
		vulnerabilidades técnicas			divulgación de información.	seguridad para el manejo de la información.
Celulares	Tecnológico	Restricción de acceso a la información	Inexistente	0-Inexistente	Restricción de acceso a la información.	Establecer políticas del uso y mantenimiento de dispositivos móviles, capacitación del personal.
Mega	Tecnológico	Prevención de fuga de datos	Inexistente	0-Inexistente	No hay prevención de fuga de datos.	Establecer políticas sobre el uso de servicios en la nube, acuerdos de confidencialidad y capacitación de personal.
Mega	Tecnológico	Requisitos de seguridad en aplicaciones	Inexistente	0-Inexistente	No hay requisitos de seguridad en aplicaciones.	Establecer políticas sobre el uso de servicios en la nube, acuerdos de confidencialidad y capacitación de personal.
Red Wifi	Tecnológico	Restricción de acceso a la	Inexistente	0-Inexistente	Vulnerabilidad por no haber restricción de	Establecer políticas para el uso de la red,

Nombre-activo	Tipo de control	Control	Estado actual	Nivel de madurez COBIT	Análisis Magerit	Recomendaciones
		información			acceso a la información.	contraseñas fuertes, capacitación de personal, control de accesos.
Contraseñas	Tecnológico	Restricción de acceso a la información	Inexistente	0-Inexistente	No existen políticas de seguridad para la prevención de acceso a la información.	Generar políticas de seguridad de contraseñas y capacitación de usuarios.
Contraseñas	Tecnológico	Prevención de fuga de datos	Inexistente	0-Inexistente	No hay prevención de fuga de datos.	Generar políticas de seguridad de contraseñas y capacitación de usuarios.
Hojas de vida de empleados	Físico	Protección contra amenazas físicas y medioambientales	Inexistente	0-Inexistente	Riesgo de pérdida o exposición física.	Digitalización y almacenamiento seguro de los documentos críticos junto a medidas físicas de protección.

Nota: Nivel de madurez.

Conclusión Evaluación de Grado de Madurez. De acuerdo a la evaluación del grado de madurez según COBIT todos los activos presentan un grado de madurez nivel 0-Inexistente, lo

cual evidencia una ausencia general de controles implementados. En análisis con la metodología Magerit, su nivel de riesgo inherente se asocia a la inexistencia de salvaguardas efectivos que reducen la probabilidad y el impacto.

Por lo anterior se recomienda:

- Implementar los controles mínimos que se indican.
- Generar documentación y responsables, con el fin de buscar el nivel 2-Gestionado.
- Planear a mediano plazo las métricas y revisiones para llegar al nivel 3-Establecido donde se busca mejorar el riesgo residual de los riesgos.

Fase 2 Conocer la Estrategia Corporativa de la Organización

La estrategia corporativa de la compañía establece algunas áreas claves:

Identificación de la Estrategia

Crecimiento y expansión: La compañía busca un crecimiento significativo en el mercado por medio de diversificación de sus servicios como la integración de diferentes medios de transporte, almacenamiento adaptable a necesidades específicas de sus clientes, esto creando alianzas estratégicas como compañías locales e internacionales.

Excelencia operativa: La empresa busca la excelencia operativa por medio de la planificación de rutas más estables y precisas que permita la reducción de costos y tiempos. Busca invertir en capacitación de personal donde se enfoquen en temas relevantes de los procesos actuales que ayuden a mejorar el manejo correcto de la operación y la atención al cliente.

Tecnología e innovación: La organización busca la automatización de sus procesos operacionales donde se pueda realizar con más confianza cada una de las actividades ya que esto

ayuda a minimizar los errores humanos. También busca establecer controles de ciberseguridad donde se implementen medidas como la segmentación de la red, implementación de un IDS, capacitaciones continuas de ciberseguridad para todos los empleados de la compañía.

Implicaciones para la seguridad

Algunas implicaciones que se pueden presentar teniendo en cuenta la estrategia corporativa de la compañía son:

Tabla 13

Implicaciones para la Seguridad

Área clave	Implicaciones de seguridad
Crecimiento y expansión	Evaluar riesgos en el compartimiento de datos al realizar alianzas estratégicas. Incluir cláusulas de seguridad y confidencialidad. Implementar medidas para la protección de datos de los clientes.
Excelencia operativa	Proteger los diferentes sistemas utilizados para la operación contra accesos no autorizados. Formación de buenas prácticas de seguridad para sus empleados. En cuanto sus clientes se debe crear canales de comunicación que ayude con la protección de suplantación de identidad.
Tecnología e innovación	Se debe busca y evaluar los riesgos en los sistemas o procesos automatizados. Segmentar la red con el finde evitar la propagación de ataques. Implementar herramientas de IDS para detectar actividades que afecten la seguridad de la información. Las capacitaciones continuas de los empleados deben ser integrales, realizando también simulacros de incidentes cibernéticos.

Nota. Implicaciones de seguridad que se pueden presentar teniendo en cuenta la estrategia corporativa de la organización.

La estrategia corporativa de la compañía evidencia un enfoque muy claro en el crecimiento del negocio, la excelencia operativa y la innovación tecnológica. Sin embrago ante estas prioridades se hace necesario incluir nuevos riesgos en materia de seguridad de la información.

El área del crecimiento y expansión indica que se hace más frecuente el intercambio de información entre compañías, esto indica que se deben tomar medidas más estrictas en el manejo de la información la cual debe ser confidencial, integra y disponible.

En cuanto a la excelencia operativa, la dependencia de sistemas tecnológicos puede llevar a interrupciones por accesos no autorizados o suplantación de identidad. Lo anterior indica la necesidad de procesos seguros y establecidos en sus políticas.

Referente a la tecnología e innovación, se evidencia la necesidad de controles de ciberseguridad, como la segmentación de la red y la implementación de un IDS/IPS.

En base a lo anterior la estrategia corporativa se ve en riesgo, por lo anterior se propone poner en práctica el plan director de seguridad diseñado el cual se encuentra alineado a la ISO 27000.

Desarrollo Objetivo 2

Diseño de políticas de seguridad (Definir políticas de seguridad amparadas bajo la normatividad ISO 27000, estableciendo protocolos aplicables a su infraestructura tecnológica y necesidades particulares de la organización).

En base a las necesidades actuales de la organización y teniendo en cuenta el análisis de sus activos en cuanto a los riesgos, amenazas y vulnerabilidades que presentan, se realiza el diseño de las políticas de seguridad buscando proteger la confidencialidad, integridad y disponibilidad de dichos activos.

Las políticas de seguridad se realizan en base a los activos mitigados los cuales buscan medidas y controles que ayuden a reducir los riesgos que presentan.

Seguido se listan las políticas de seguridad diseñadas para la empresa, la especificación de estas políticas se encuentra en el anexo **(*Políticas de seguridad- .docx*):**

Tabla 14

Lista de Políticas de Seguridad

Política	Propósito
Política de control de accesos - Computadores	Implementar controles para la gestión de acceso a los computadores, garantizando que sean utilizados por el personal autorizado según los roles y permisos asignados con el fin de minimizar el riesgo de accesos no autorizado.
Política de actualizaciones de software y sistemas operativos - Computadores	Establecer lineamientos y procedimientos para la actualización de software, sistemas operativos y dispositivos de la organización, buscando minimizar el riesgo asociado a las vulnerabilidades.
Política de dispositivos móviles - Celulares	Establecer reglas y procedimientos para el uso de dispositivos móviles buscando proteger la información confidencial y minimizar los riesgos relacionados al uso indebido de dispositivos móviles.
Política de gestión de antivirus - Software	Establecer las políticas y procedimientos para la instalación, configuración y actualización de antivirus, buscado proteger los sistemas de la información.
Política para plataformas de almacenamiento en la nube	Establecer directrices claras con el fin de garantizar el acceso seguro a las plataformas de almacenamiento en la nube, minimizando los riesgos no autorizados y protegiendo la confidencialidad, integridad y disponibilidad de la información.
Políticas de respaldo- plataformas de almacenamiento en la nube	Establecer directrices para garantizar la confidencialidad, integridad y disponibilidad de la información que se almacena en la nube por medio de respaldos y almacenamiento seguro.
Políticas de confidencialidad firma obligatoria	Establecer directrices para proteger la información sensible de

Política	Propósito
de acuerdos de confidencialidad para todos los empleados de la compañía-Personal empleados	la organización por medio de una firma obligatoria de acuerdos de confidencialidad.
Políticas de creación y gestión de contraseñas	Establecer los requisitos mínimos para la creación, uso y la gestión segura de las contraseñas, buscando garantizar la protección de la información contra accesos no autorizados.
Políticas de monitoreo en el tráfico de red	Establecer lineamientos para la supervisión continua del tráfico de red con el fin de identificar accesos no autorizados y posibles incidentes de seguridad.

Nota: Tabla donde se indica el listado de las políticas de seguridad diseñadas.

El diseño de las políticas de seguridad se realiza en base a las brechas de seguridad identificadas, haciendo relación entre la valoración del riesgo y la definición de medidas preventivas.

La selección de políticas seleccionadas en las áreas de control de accesos, gestión de contraseñas, uso de dispositivos móviles y plataformas en la nube muestran la priorización de los activos más críticos.

Las políticas de seguridad diseñadas establecen lineamientos operativos y un marco normativo interno alineado a la norma ISO 27000, reduciendo las vulnerabilidades y fortaleciendo la capacidad de respuesta de la organización. La disponibilidad y detección temprana de incidentes que se evidencian en las políticas del monitoreo de trafico de red y la del respaldo en la nube, muestran un paso importante en la construcción de un sistema integral de seguridad.

Se requiere que, las políticas de seguridad diseñadas se acompañen con mecanismos de implementación, seguimiento y capacitación del personal.

Este conjunto de políticas de seguridad construye un avance solido con el fin de cubrir los vacíos de seguridad que presenta la compañía, las políticas de seguridad deben ser aplicadas con el fin de poder contribuir efectivamente a la protección de la información, dando cumplimiento a las normas establecidas.

Fase 3 Definir los Proyectos de Seguridad

Para el diseño del plan director de seguridad para la empresa se hace necesario establecer algunos proyectos de seguridad estratégicos que permitan abordar las necesidades que se han identificado por medio de los análisis realizados anteriormente y alineándolos a los objetivos corporativos. La definición de estos proyectos permite mitigar los riesgos asociados a las ciber-amenazas y garantizar la continuidad del negocio protegiendo la información crítica de la organización.

Los proyectos propuestos buscan priorizar la mitigación de los riesgos encontrados por medio de controles básicos de seguridad como políticas de seguridad, capacitaciones y algunas tecnologías.

A continuación, se presentan los proyectos propuestos, los cuales son una iniciativa que representa los primeros pasos para construir un entono digital confiable que proteja los activos de información de la organización.

Proyecto 1 – Inventario y clasificación de Activos de Información

Objetivo. Establecer un inventario completo y detallado de todos los activos de información que se manejan en la compañía, garantizando que cada activo sea identificado, documentado y clasificado según su riesgo de seguridad.

Justificación. La ausencia de un inventario de activos crea una de las principales brechas de seguridad, ya que no permite la identificación de los riesgos y la implementación de controles

efectivos. Con un inventario actualizado, la compañía podrá priorizar inversiones en seguridad y establecer controles técnicos.

Actividades Principales

Identificación de Activos. Se debe realizar por medio de levantamiento de información en toda la organización con el fin de identificar activos críticos.

Documentación de Inventario. Se debe crear una base de datos donde se almacene la información detallada de cada activo con datos como (Nombre, tipo de activo, ubicación, responsable, fecha de adquisición), entre otros.

Clasificar los Activos. Los activos deben ser clasificados según su un nivel de criticidad (Media, alta, baja), considerando el impacto de la confidencialidad, integralidad y disponibilidad de la información.

Validación y Actualizaciones. Se debe realizar una revisión y actualización regular del inventario.

Resultado Esperado. Un repositorio centralizado y detallado que permita la gestión y protección correcta de los activos de información reduciendo los riesgos asociados a accesos indebidos y perdidas de datos.

Proyecto 2 – Políticas de Seguridad de la Información

Objetivo. Implantar directrices, normas y responsabilidades que permitan proteger los activos de información de la compañía contra amenazas internas y externas, asegurando la confidencialidad, integridad y disponibilidad de la información.

Justificación. La ausencia de políticas de seguridad crea una brecha muy significativa para la organización, causando incidentes de seguridad que pueden comprometer la información de la compañía y sus clientes. Las políticas de seguridad constituyen un requisito normativo

alineado a la norma ISO 27000 y un requisito de instrumento estratégico con el fin de reducir las vulnerabilidades, estandarizar prácticas de seguridad y fomentar la responsabilidad compartida en la protección de la información.

Actividades Principales. Análisis de requisitos: Identificar las necesidades específicas de la organización referente a sus activos de información y en base al análisis de riesgo que presentan con el fin de determinar los activos que requieren protección.

Diseño de la política: Diseñar un documento con políticas de seguridad para los activos de información donde defina el propósito, sus directrices, roles y responsabilidades, cumplimiento entre otros.

Aprobación y Comunicado. Se debe contar con la aprobación por parte de la gerencia con lo cual se busca asegurar el cumplimiento de las políticas las cuales serán comunicadas posteriormente a toda la organización.

Implementación. Se debe poner en práctica las políticas de seguridad diseñadas, tanto sus controles técnicos y administrativos.

Monitoreo: Se debe monitorear constantemente el cumplimiento de la política de seguridad por medio de auditorías internas y analizando incidentes de seguridad que se presenten.

Resultado Esperado. La compañía contara con un marco normativo que ayudara a minimizar el riesgo que enfrentan sus activos de información.

Proyecto 3 – Fortalecimiento de la Red Corporativa

Objetivo. Fortalecer la seguridad de la red corporativa mediante la implementación de medidas que prevengan accesos no autorizados, segmentando la red adecuadamente y optimizando las capacidades de detección y repuesta ante amenazas de manera oportuna.

Justificación. El análisis de riesgo evidencio que la red Wifi y los servicios de comunicación representan activos de comunicación representan activos de alta criticidad, al no contar con una rede segmentada y mecanismos de monitoreo.

El fortalecimiento es una acción estratégica que busca garantizar la confidencialidad, integridad y disponibilidad de los datos, alineadas con la norma ISO 27001. Este proyecto contribuye a cerrar las brechas de seguridad más significativas, asegurando que los procesos de la organización se desarrollen sobre una infraestructura confiable.

Actividades Principales

Configuración de Cortafuegos. Seleccionar un firewall adecuado y establecer reglas de acceso con el fin de permitir solo tráfico autorizados y configurando filtros que bloqueen accesos sospechosos.

Segmentar la Red. Identificar las áreas claves de la organización con el fin de definir las áreas claves que deben ser segmentadas como administración, empleados y visitantes.

Implementación de un IDS/IPS: Evaluar la implementación de un IDS/IPS de código abierto (Snort, Suricata, Zeek) o comerciales.

Resultado Esperado

Mediante el fortalecimiento de la red, la compañía espera minimizar los accesos no autorizados, reduciendo fugas de información, mejorar el control y la gestión de la red, facilitando el monitorio de posibles amenazas.

Fase 4 Clasificar y Priorizar Proyectos

Esta fase donde se realiza la clasificación y priorización de proyectos para la organización se fundamenta en el análisis realizado a la situación actual de la empresa y aplicando criterios a la mitigación de los riesgos críticos y al impacto que presentan.

La clasificación de estos proyectos no solo tiene que ver con un criterio técnico, sino también a una viabilidad económica, de personal y la dependencia de proveedores externos. De esta manera, se garantiza que los proyectos prioritarios como el inventario de activos, la definición de políticas de seguridad y el fortalecimiento de la red corporativa, sean ejecutados en etapas tempranas.

Evaluación de los Proyectos de Seguridad

Para la evaluación de los proyectos de seguridad es de gran importancia evaluar lo siguiente:

Mitigación de Riesgos. Por medio de este criterio se evalúa la contribución el proyecto tiene en la reducción de los riesgos más críticos de la organización.

Esfuerzo vs. Impacto. Se realiza la comparación de la cantidad de recursos y el tiempo para la implementación.

Alineación Estratégica. Se analiza si el proyecto esta alineado a los objetivos estratégicos de la organización y si se cumple con requisitos normativos o estándares de seguridad.

Costos y Recursos. Se evalúa el nivel de inversión económica para ser ejecutados.

Prioridad. Se indica que tan necesario y urgente es la implementación del proyecto.

Tabla 15

Proyectos de Seguridad

Proyecto	Mitigación de riesgos	Esfuerzo vs. Impacto	Alineación estratégica	Costos y recursos	Prioridad
Inventario y clasificación de activos de información	Alta (El inventario es la base para identificar los activos que están en riesgo)	Moderado-Alto (Se requiere de un trabajo y tiempo entre las diferentes áreas).	Muy alto (Se encuentra lineado con la ISO 27001).	Moderado (No requiere de inversión económica, pero si del tiempo del personal).	Alta
Políticas de seguridad de la información	Moderado (Establece reglas que permiten proteger los activos).	Bajo-Alto (Se requiere de esfuerzo para la creación de las políticas, pero genera un impacto significativo).	Muy alto (Su requisito fundamental alinea los estándares y establece una cultura de seguridad).	Moderado (Se requiere de tiempo del personal directivo y de un equipo o personal de seguridad para desarrollarlas.)	Alta
Fortalecimiento de la red corporativa	Muy alto (Reduce las vulnerabilidades que presenta la infraestructura de la red, evitando ataques	Alto-Alto (Requiere de recursos técnicos para su planificación e implementación, pero su impacto	Alto (Asegura la operatividad diaria de la compañía permitiendo alcanzar sus	Alto (Se requiere de una inversión tecnológica).	Alta

	cibernéticos, fugas de información y accesos no autorizados).	es significativo para la seguridad de la red).	objetivos de seguridad).

Nota: Proyectos de seguridad propuestos para el plan director de seguridad.

Basado en el análisis anterior se concluye que el orden y la priorización de los proyectos se dan de la siguiente manera:

Proyecto - Políticas de seguridad de la información: Presenta un moderado costo y esfuerzo, pero presenta un alto impacto y alineación estratégica.

Proyecto - Inventario y clasificación de activos de información: Presenta un esfuerzo moderado, se considera como segundo paso lógico después de definir y establecer las políticas de seguridad.

Proyecto - Fortalecimiento de la red corporativa: Su importancia es muy relevante para la mitigación de riesgos críticos, pero requiere más recursos y debe ser implementada después de los proyectos anteriores con el fin de garantizar su eficiencia.

Fase 5 Aprobación del Plan Director de Seguridad

Esta fase busca la aprobación formal por parte de la gerencia del plan director de seguridad, antes de pasar por diferentes revisiones y ajustes pertinentes.

La dirección realiza el análisis del alance, la duración y la prioridad de los proyectos definidos, y es posibles que se soliciten ajustes. Después de que se realicen ajustes al documento este debe pasar nuevamente por revisión, este proceso puede repetirse varias veces hasta lograrla aprobación por parte de la gerencia o dirección de la empresa.

Fase 6 Implementación del Plan director de Seguridad

Dado a las condiciones ejecutables del proyecto y del alcance de este, la fase 6 no será desarrollada. Pero a continuación se propone un plan de continuidad con el fin de que la compañía ponga en marcha el plan director de seguridad diseñado.

Estrategia de Continuidad del Plan Director de Seguridad

Propósito. Con el fin de asegurar la sostenibilidad el plan director de seguridad diseñado para la compañía y garantizar que las acciones propuestas trasciendan la etapa de diseño y aprobación hacia la ejecución en un entorno real. Con la ejecución de este plan director de seguridad se busca fortalecer la cultura organizacional en cuanto a la seguridad informática, reduciendo la exposición al riesgo y consolidando una gestión integral de la información alineadas a la norma ISO 27001.

Objetivos de la Estrategia. Implementar de manera progresiva los controles y políticas de seguridad diseñados en este plan director de seguridad.

Establecer un sistema de seguimiento que permita medir el grado de madurez de la seguridad información en la compañía.

Fortalecer la cultura organizacional en la seguridad informática, por medio de capacitaciones continuas.

Plan de implementación

Tabla 16

Plan de Implementación

Fase	Acción	Responsable	Plazo estimado
Socialización y validación	Presentar y socializar el plan director de seguridad a la alta dirección y equipos.	Gerencia general	Mes 1
Priorización y asignación de recursos	Definir prioridades de implementación según la criticidad de los activos, riesgo y disponibilidad de recursos.	Dirección TI/Gerencia	Mes 2
Implementación de controles	Poner en ejecución los planes de acción definidos en este plan director de seguridad como las políticas de seguridad, procedimientos y controles.	Dirección TI/Gerencia	Mes 3-6
Monitoreo y evaluación	Realizar auditorías internas de cumplimiento.	Dirección TI/Gerencia	Mes 7
Ajustes y mejoras	Realizar análisis a los resultados, corrigiendo y fortaleciendo los controles implementados.	Dirección TI/Gerencia	Mes 8 en adelante

Nota: Fases para la implementación del plan director de seguridad.

Mecanismos para Seguimiento y Evaluación. Con el fin de garantizar la efectividad de la estrategia, se recomienda lo siguiente:

Generar Indicadore de Desempeño. Generar indicadores en porcentaje de controles implementados respecto al total planificados.

Indicador que permita ver la reducción porcentual de incidentes de seguridad.

Herramientas de Control. Reuniones mensuales del comité de seguridad

Auditorías internas semestrales

Informes de seguimiento y actualización del plan director de seguridad.

La ejecución de esta estrategia permitirá visualizar el impacto del plan director de seguridad, mostrando las mejoras en el nivel de madurez, el cumplimiento normativo y la mitigación del riesgo. De igual manera ayuda a consolidar una cultura orientada a la seguridad informática, garantizando la continuidad del negocio y la protección de los activos de información de la compañía.

Desarrollo Objetivo 3

Desarrollar un plan de formación en seguridad de la información, que incluya un manual de funciones y responsabilidades, orientado a promover buenas prácticas y asegurar la correcta aplicación de políticas de establecidas.

Fundamento del Plan de Formación

Diversos estudios han demostrado que la gran mayoría de incidentes de seguridad tiene origen en errores humanos ya que hay una ausencia de cultura organizacional, esto ha generado que el factor humano sea catalogado como uno de los principales vectores de riesgo en la seguridad informática. (Solano et al., 2016)

En la compañía se ha identificado algunas brechas críticas de seguridad relacionadas con el desconocimiento de amenazas como phishing y malware, el uso inadecuado de contraseñas, la carencia de protocolos de seguridad y la carencia de mecanismos para el reporte de incidentes de seguridad, incrementando por medio de estas brechas la probabilidad de accesos no autorizados, fugas de información y afectación a la continuidad del negocio.

Con el objetivo de fortalecer una cultura organizacional de seguridad de la información para la compañía, se plantea un plan de formación y capacitación en seguridad de la información. Este plan contiene un manual de funciones de ciberseguridad, el cual define las responsabilidades y mejores prácticas que cada rol dentro de la compañía debe cumplir con el fin de garantizar la protección de la información y el cumplimiento de las políticas de seguridad establecidas o diseñadas.

Metodología de Formación

Este plan de formación se basa en una metodología mixta que integra una formación teórica, practica y evaluativa, con la cual se busca garantizar una apropiación integral de

conocimientos por parte de los empleados y su aplicación en el mundo laboral.

La metodología se compone de lo siguiente:

Formación teórica: La formación teórica contempla sesiones virtuales tipo webinar orientadas a la concientización y la comprensión de conceptos fundamentales de seguridad, como amenazas, políticas internas y buenas prácticas.

Formación práctica: Talleres y ejercicios aplicados que permiten realizar ejercicios en escenarios reales, como son la identificación de phishing, manejo de contraseñas seguras y el manejo de incidentes de seguridad.

Refuerzo continuo: Se propone realizar un refuerzo periódico con recordatorios, capsulas informativas y material de consulta sobre la seguridad en la organización.

Evaluaciones: En cuanto a las evaluaciones se propone realizar aplicación de pruebas de conocimiento y encuestas de percepción, antes y después de cada formación.

Las capacitaciones se realizan como parte del proceso de inducción de nuevos empleados, con refuerzos trimestrales y una actualización anual para toda la organización.

Vinculo del Plan de Formación con los Riesgos de Seguridad de la Información

El plan de formación fue establecido teniendo en cuenta las brechas de seguridad identificadas en la organización:

Tabla 17

Modulo-Riesgo-Control

Módulo de formación	Riesgo mitigado	Control aplicado
Concientización y seguridad de la información	Toma de conciencia de seguridad	Capacitación básica y campañas de sensibilización.
Uso seguro de contraseñas y autenticación	Accesos no autorizados	Políticas de contraseñas y autenticación multifactor
Phishing y amenazas en el correo electrónico	Robo de credenciales	Simulaciones o experimentos controlados
Protección de datos y acceso a la información	Fugas de información	Clasificación de información y controles de acceso
Manejo de dispositivos y teletrabajo	Conexiones inseguras	Uso de VPN y buen uso de dispositivos
Manejo de incidentes de seguridad	Respuesta tardía a incidentes	Reporte y manejo de incidentes de seguridad

Nota: Relación entre plan de formación y riesgos

Lo anterior muestra la necesidad de aplicar el plan de formación el cual ayudara con el control organizacional alineado a la gestión de los riesgos, y contribuyendo a la mitigación de las amenazas más relevantes.

Con Relación a la ISO 27001

Con relación a la ISO 27001 existen temas relacionados con la concientización, educación y capacitación en seguridad informática donde se sugieren temas como(ISO/CEI, n.d.).

Un amplio grupo de empleados proveedores y contratistas deben conocer elementos

básicos como (políticas de seguridad de la información, como pueden contribuir a proteger la información. Etc.)

Muestra la necesidad de concienciar y capacitar al personal en temas de seguridad de la información.

Muestra la relación de roles y responsabilidades las cuales deben ser claras.

Funciones de Funciones de Ciberseguridad

El manual de funciones de ciber seguridad indica las responsabilidades y las acciones preventivas de cada rol, donde se garantiza una adecuada gobernanza de la seguridad de la información.

Tabla 18

Roles y Funciones

	Funciones	Acciones preventivas
Administrativo	Aprueba y supervisa el plan de formación y capacitación. Define y actualiza las políticas de seguridad de la información. Asigna recursos para la ejecución del plan. Gestionar auditorías internas y externas.	Verifica la asistencia a las capacitaciones. Valida la aplicación de políticas de controles. Coordina las respuestas ante incidentes.
Operaciones	Cumplir con las políticas de seguridad establecidas. Reportar los incidentes de seguridad. Proteger la información operativa. Participar de las capacitaciones.	Aplicar buenas prácticas en contraseñas y dispositivos. Realizar copias de seguridad.
Comercial	Proteger la información de clientes y proveedores. Cumplir normativa de privacidad y confidencialidad. Reportar correos sospechosos y de fraude.	No compartir información por canales no autorizados.

Nota: Roles y funciones a nivel empresarial.

Viabilidad Técnica

La implementación de este plan de formación es totalmente viable, la compañía cuenta con los recursos mínimos para llevar a cabo este plan.

Para la ejecución del plan no interfiere en tiempo extralegal de los empleados ya que se realizarán dentro del horario legal y en tiempos cortos. Adicional los costos asociados al plan son moderados ya que las conferencias se realizan de manera virtual y con los recursos internos de la

compañía.

Beneficios del Plan de Formación

Fomentar las competencias del personal mediante actividades de formación y capacitación.

Promover una cultura de seguridad sostenible, asegurando la protección de la información en todos los empleados de la organización.

Crear en los empleados la capacidad de identificar y prevenir amenazas de seguridad, especialmente en ataques de ingeniería social.

Reducir los riesgos asociados al factor humano, garantizando por medio de las políticas y controles establecidos.

El desarrollo de este plan de formación y capacitación que incluye el manual de funciones de ciberseguridad, temas de formación, cronograma de formación, evaluación y formación del impacto y su implementación; se encuentra en el Anexo: Plan de formación y capacitación- SelotransSAS.docx.

Conclusiones

El diseño del plan director de seguridad para la empresa ha permitido establecer estrategias efectivas para la protección de la información. Por medio de un análisis de las brechas de seguridad se identificaron vulnerabilidades críticas, deficiencias en las políticas de seguridad y prácticas incorrectas de seguridad.

El análisis de seguridad realizado a los 16 activos de información se identificaron 29 amenazas y vulnerabilidades de las cuales, 37.93% presentan un riesgo bajo, el 44.83% presenta un riesgo apreciable, el 10.34% un riesgo importante y el 6.90% presenta un riesgo crítico. Lo anterior demuestra la importancia de conocer las brechas de seguridad y la importancia de contar con un diagnóstico detallado para la toma de decisiones.

El 17.24% de las amenazas y vulnerabilidades presentan riesgo de importante y crítico, lo cual genera un impacto significativo en la seguridad de la información de la compañía.

De las 29 amenazas y vulnerabilidades encontradas en los 16 activos de información, el 100% carece de controles adecuados, como planes de mantenimiento o políticas de seguridad, lo cual incrementa la exposición de la organización a ciberataques. Por lo anterior se recomienda la implementación de controles y políticas de seguridad diseñadas y alineadas a la norma ISO 27001.

El análisis de las brechas de seguridad y referente a los riesgos, teniendo en cuenta las 29 amenazas y vulnerabilidades identificadas en los 16 activos de información, se observa que el 58,62% de los riesgos tienen una aceptación moderada (M), lo que sugiere medidas de mitigación con el fin de reducir su impacto y probabilidad. Un 37,93% de los riesgos son inaceptables (I), lo cual indica que estos riesgos deben ser tratados de manera inmediata. Solo un 3,45% de los riesgos son aceptables (A), lo cual indica que la seguridad actual de la compañía no

es óptima y se requieren de acciones optimas de seguridad.

En cuanto a la evaluación de los riesgos asociados a las 29 amenazas y vulnerabilidades. Como análisis del tratamiento del riesgo, se determinó que el 20,69% de los riesgos (6 de 29) serán transferidos, el 48,28% (14 de 29) serán aceptados y el 31,03% (9 de 29) serán mitigados.

Al realizar el análisis de los activos de información y tomando como base 10 riesgos con estado inaceptables, se determinó que el 90% de los riesgos presenta un nivel alto y solo un 10% un nivel bajo, lo que indica que existe una vulnerabilidad significativa donde se recomienda la priorización de medidas de seguridad en accesos no autorizados, credenciales débiles, divulgación de información y configuraciones incorrectas en plataformas compartidas.

Se genera documento con un avance del 100% de políticas de seguridad, tomando como base los riesgos altos que presenta la compañía en cuanto a la seguridad de su información, cumpliendo con el objetivo del diseñar políticas de seguridad alineadas a la norma ISO 27000.

Se desarrollan las cinco fases del plan director de seguridad en un 100% lo cual representa un avance estratégico para la compañía, cumpliendo con el objetivo general.

Glosario

Ciberseguridad

ISACA define a la ciberseguridad como la Protección de activos de información, por medio del tratamiento de amenazas y que ponen en riesgo la información.

La ciberseguridad busca garantizar la protección de los activos de una organización y usuarios.

Seguridad de la Información

La seguridad de la información busca proteger los sistemas y datos de amenazas que pongan en riesgo la información.

La seguridad de la información busca reducir los riesgos y es por esta razón que se busca medidas que permitan salvaguardar la información de manera segura.

Pilares de la Seguridad de la Información

Según la ISO 27001 existen tres pilares en la seguridad de la información que son confidencialidad, disponibilidad e integralidad con los cuales se busca garantizar la adecuada gestión de la información.

Confidencialidad: Hace referencia a la calidad de la información y se busca que esta sea exacta, completa y que no presente ninguna alteración.

Disponibilidad: Hace referencia a que la información debe estar siempre disponible y accesible en el momento adecuado y desde cualquier medio tecnológico.

Integridad: Busca que la información no se encuentre alterada y no tenga modificaciones que alteren su validez.

Referencias Bibliográficas

A New Age of Cybersecurity Culture - KPMG Colombia. (2025). https://kpmg.com/co/es/home/insights/2025/01/a-new-age-of-cybersecurity-culture.html

Aceves, I. (n.d.-a). Principios de Seguridad de la Información. *Roa.Uveg.Edu.Mx*.

Aceves, I. (n.d.-b). Principios de Seguridad de la Información. *Roa.Uveg.Edu.Mx*. http://roa.uveg.edu.mx/repositorio/licenciatura2015/237/PrincipiosdeSeguridaddelaInformacin.pdf

Álvarez, C. (2023). *Colombia registró un crecimiento de ataques informáticos en el último año*. Voz de América. https://www.vozdeamerica.com/a/colombia-registro-crecimiento-ataques-informaticos-ultimo-ano-/6916577.html

Andrés Jiménez-Almeira, G., & López, D. E. (2023). Ciberseguridad y Seguridad Integral: un análisis reflexivo sobre el avance normativo en Colombia. In *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*.

Andrew Jaquith. (n.d.). *Security Metrics - Andrew Jaquith - Google Books*. Retrieved November 19, 2024, from https://books.google.es/books?lr&id=Af8F00gTRN4C&oi=fnd&pg=PT15&dq=%22Security+Metrics:+Replacing+Fear,+Uncertainty,+and+Doubt%22&ots=NrkTpr-QuK&sig=k3oIHArGbpcJK-jbO6jXest6euU&hl=es&pli=1#v=onepage&q&f=false

Arcos-Argudo, M., Matute-Pinos, K., & Fernández-Mora, M. (2023). Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación colombiana desde un enfoque de ciberseguridad y delitos informáticos. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *2023*(E60).

Arroyabe, M. F., Arranz, C. F. A., De Arroyabe, I. F., & Fernandez de Arroyabe, J. C. (2024).

Navigating Cybersecurity: Environment's Impact on Standards Adoption and Board Involvement. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2024.2394440/ASSET/F37A628A-6D13-46FF-9DA5-56E8B96531C4/ASSETS/GRAPHIC/UCIS_A_2394440_F0006_B.GIF

Barraza de la Paz, J. V., Rodríguez-Picón, L. A., Morales-Rocha, V., & Torres-Argüelles, S. V. (2023). A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0. *Systems*, *11*(5), 1–19.

Christian, P., & Ochoa, B. (2018). *IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN, RIESGOS Y CONTROLES ASOCIADOS PARA LA EMPRESA ESTRATEGIAS EMPRESARIALES DE COLOMBIA BAJO LA NORMA ISO 27001 E ISO 31000*.

Ciberseguridad, I. nacional de. (n.d.). Plan director de seguridad. *Incibe*.

Cloudflare. (n.d.). *Qué es la seguridad de la información | Cloudflare*. Retrieved May 3, 2024, from https://www.cloudflare.com/es-es/learning/security/what-is-information-security/

Congreso de Colombia. (2012). *Ley 1581 de 2012 (Octubre 17)*. 1–9.

coordinación de contenidos, E., General de Modernización Administrativa, D., & Impulso de la Administración Electrónica, P. (2012). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*. http://administracionelectronica.gob.es/

Davies, S. J., & Fennelly, L. J. (2019). The professional protection officer: Practical security strategies and emerging trends. In *The Professional Protection Officer: Practical Security Strategies and Emerging Trends*. https://doi.org/10.1016/C2018-0-01136-6

Diéguez, M., Cares, C., Cl, M. D., & Cl, C. C. (n.d.). *Comparación de dos enfoques cuantitativos para seleccionar controles de seguridad de la información*.

https://doi.org/10.17013/risti.32.113-128

Eito-Brun, R., & Calleja Aliaga, C. (2020). La gestión documental en los modelos de gobernanza TIC: presencia y visibilidad de la normativa internacional en el modelo de referencia COBIT. *Revista Española de Documentación Científica*, *43*(3). https://doi.org/10.3989/redc.2020.3.1666

Epa, U. S., & Information, E. (2016). *Information Security – Roles and Responsibilities Procedures*. 1–32.

Fabiana Meijon Fadul. (2019). *Integridad de los datos*.

Fortiguard. (2024). *Cyberthreat Predictions for 2024 An Annual Perspective from FortiGuard Labs*.

Gallardo, E. (2017). Metodología de la Investigación. *Universidad Continental*, *1*, 98.

Gonzáles, J., & Méndez, J. (2021). *Diseño del Plan Director de Ciberseguridad para las aplicaciones expuestas en internet por el Banco Agrario de Colombia basado en la norma ISO/IEC 27032:2012*. 1–173.

Hostetler, C., & Hostetler, C. (2011). *Plan director*. 2011.

IBM. (2023). *¿Qué es el ransomware? | IBM*. https://www.ibm.com/es-es/topics/ransomware

Ibrahim, A. I. G. (2021). Cybersecurity: Panorama and Implementation in 2021. *WIT Transactions on the Built Environment*, *206*, 41–54. https://doi.org/10.2495/SAFE210041

Icontec. (2022). *Norma tecnica colombiana NTC-ISO/IEC 27001*. 25.

INCIBE. (n.d.). Plan director de Seguridad. *INSTITO NACIONAL DE CIBERSEGURIDAD*.

Infosecurity. (n.d.). *Ciberseguridad*. Retrieved May 3, 2024, from https://www.infosecuritymexico.com/es/ciberseguridad.html

Kassa, S. G. (2017). IT asset valuation, risk assessment and control implementation model. *Journal*

Risk Management, *3*(8), 125–134.

Kizza, J., & Migga Kizza, F. (2011). Digital Evidence and Computer Crime. In *Securing the Information Infrastructure*. https://doi.org/10.4018/978-1-59904-379-1.ch015

Kosinski, M. (2024). *¿Qué es el phishing? | IBM*. IBM. https://www.ibm.com/es-es/topics/phishing

Lella, I. (n.d.). *ENISA THREAT LANDSCAPE 2023*. https://doi.org/10.2824/782573

López, R. (2017a). Sistema de Gestión de la Seguridad. In *Fundación Universitaria del Área Andina*.

López, R. (2017b). Sistema de Gestión de la Seguridad. In *Fundación Universitaria del Área Andina*. https://digitk.areandina.edu.co/handle/areandina/1238

Lundgren, B., & Möller, N. (2017). Defining Information Security. *Science and Engineering Ethics*, *25*(2), 419. https://doi.org/10.1007/S11948-017-9992-1

Mamami, R. G. R., Ancco, R. C., & Argollo, R. R. L. (2023). Política de TI y gestión de seguridad de la información basada en ISO 27 001. *Innovación y Software*, *4*(1), 96–106. https://doi.org/10.48168/innosoft.s11.a57

Margi Van Gogh, Felipe Beato, L. R. (2024). *Por qué debemos hacer que el transporte y las cadenas de suministro sean ciberseguras | Foro Económico Mundial*. World Economic Forum. https://www.weforum.org/agenda/2024/06/transport-supply-chain-ecosystems-cyber-resilience/

Miranda, E. E. R. (2019). *"SGSI BAJO EL MARCO NORMATIVO ISO 27001 EN EL PROCESO DE CONTROL DE ACCESOS PARA UNA EMPRESA: una revisión científica de los últimos 9 años."*

Mosquera Amancio, V. (n.d.). *CIBERSEGURIDAD EN COLOMBIA*.

Outpu, I. (2021). *What are Information Security Controls?* Input Output.

https://www.inputoutput.com/blog/what-are-information-security-policies-and-procedures

Pender-Bey, G. (n.d.). *THE PARKERIAN HEXAD The CIA Triad Model Expanded*.

Rawat, P. (2023a). *Fundamental Principles of Information Security - InfosecTrain*. INFONSECTRAIN. https://www.infosectrain.com/blog/fundamental-principles-of-information-security/

Rawat, P. (2023b). *Fundamental Principles of Information Security - InfosecTrain*. INFONSECTRAIN. https://www.infosectrain.com/blog/fundamental-principles-of-information-security/

Ritegno, E. (2018). COBIT es el marco de trabajo reconocido a nivel mundial, que ayuda a garantizar el Gobierno Corporativo de la Información y la Tecnología (GEIT) © 2018. *Isaca*, 43.

Rodriguez, A., & Andrés, Y. (2016). Entendiendo el SGSI. *Universidad Piloto de Colombia*, 1–7.

Smowl. (2024). *Vulnerabilidad en la seguridad informática: qué es, definición, tipos y consejos*. Https://Smowl.Net/Es/Blog/Vulnerabilidad-En-La-Seguridad-Informatica/. https://smowl.net/es/blog/vulnerabilidad-en-la-seguridad-informatica/

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: a historical and conceptual review. *International Journal of Information Security*, *23*(3), 1695–1719. https://doi.org/10.1007/s10207-023-00811-x

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *22*, 73–88. https://doi.org/10.17013/risti.22.73-88

Valkenburg, B., & Bongiovanni, I. (2024). Unravelling the three lines model in cybersecurity: a

systematic literature review. *Computers and Security*, *139*. https://doi.org/10.1016/j.cose.2024.103708

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/J.COSE.2013.04.004

WORLD, T. L. (2024). *Cómo proteger el transporte contra amenazas cibernéticas*. The Logistics World. https://thelogisticsworld.com/transporte/ciberseguridad-en-el-transporte-retos-y-soluciones-para-proteger-las-operaciones-logisticas/

Apéndices

Apéndice A

Análisis de Riesgo

Matriz Análisis de Riesgos - SelotransSAS2.xlsx (Matriz Analisis de Riesgos-V2.xlsx)

Apéndice B

Informe Brechas de Seguridad

Informe-DiagnosticoBrechas de seguridad.docx (Informe-DiagnosticoBrechas de seguridad.docx)

Apéndice C

Políticas de Seguridad

Políticas de seguridad.docx (Politicas de seguridad.docx)

Apéndice D

Plan de Capacitación

Plan de formación y capacitación.docx (Plan de formación y capacitación.docx)

Apéndice E

Carpeta de Trabajo

Trabajo de grado-Claudia Gallego